Official Journal
of the European Union

IS
L Series

2024/1689

12.7.2024

REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

June 13, 2024

establishing harmonised rules on artificial intelligence and amending Regulations (EC) No. either300/2008, (EU) n.either167/2013, (EU) n.either168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Regulation)

(Text with EEA relevance)

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,

Following 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 European Central Bank [2],

Having regard to the opinion of the Committee of the Regions [3],

In accordance with the ordinary legislative procedure [4],

Considering the following:

(1) The objective of this Regulation is to improve the functioning of the internal market by establishing a uniform legal framework, in particular for the development, placing on the market, putting into service and use of artificial intelligence systems ('AI systems') in the Union, in accordance with Union values, in order to promote the uptake of human-centred and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety and fundamental rights enshrined in the Charter of Fundamental Rights of the European Union ('the Charter'), including democracy, the rule of law and environmental protection, protecting against harmful effects of AI systems in the Union, as well as supporting innovation. This Regulation ensures the free cross-border movement of goods and services based on AI, thereby preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless expressly authorized by this Regulation.

(2) This Regulation should be implemented in accordance with the Union values as enshrined in the Charter, facilitating the protection of natural persons, businesses, democracy, the rule of law and environmental protection, while boosting innovation and jobs and making the Union a leader in the adoption of trustworthy AI.

(3) AI systems can be easily deployed in a wide range of sectors of the economy and in many parts of society, including across borders, and can easily circulate throughout the Union. Some Member States have already considered adopting national rules to ensure that AI is trustworthy and safe and is developed and used in compliance with fundamental rights obligations. Diverging national rules may lead to fragmentation of the internal market and reduce legal certainty for operators developing, importing or using AI systems. A high and consistent level of protection across the Union should therefore be ensured in order to achieve trustworthy AI, and divergences that hinder the free movement, innovation, deployment and adoption of AI systems and AI systems in the internal market should be avoided.

[1] OJ C 517 of 22.12.2021, p. 56.

[2] OJ C 115 of 11.3.2022, p. 5.

[3] OJ C 97 of 28.2.2022, p. 60.

[4] Position of the European Parliament of 13 March 2024 (not yet published in the Official Journal) and decision of the Council of 21 May 2024.

products and related services by establishing uniform obligations for operators and ensuring uniform protection of overriding purposes of general interest and of the rights of individuals throughout the internal market, on the basis of Article 114 of the Treaty on the Functioning of the European Union (TFEU). To the extent that this Regulation contains specific rules for the protection of individuals with regard to the processing of personal data restricting the use of AI systems for remote biometric identification for law enforcement purposes, the use of AI systems for risk assessments of natural persons for law enforcement purposes and the use of AI systems for biometric categorisation for law enforcement purposes, it is appropriate to base this Regulation, as regards those specific rules, on Article 16 TFEU. In the light of those specific rules and the recourse to Article 16 TFEU, it is appropriate to consult the European Data Protection Board.

(4) AI is a rapidly evolving set of technologies that contribute to a wide range of economic, environmental and social benefits across all economic sectors and societal activities. The use of AI can provide essential competitive advantages to businesses and facilitate positive social and environmental outcomes in healthcare, agriculture, food safety, education and training, media, sport, culture, infrastructure management, energy, transport and logistics, public services, security, justice, resource and energy efficiency, environmental monitoring, biodiversity and ecosystem conservation and restoration, and climate change mitigation and adaptation, among others, by improving prediction, optimising operations and resource allocation, and personalising digital solutions available to people and organisations.

(5) At the same time, depending on the circumstances relating to its application, use and level of technological development, AI may create risks and undermine public interests and fundamental rights protected by Union law. Such damage may be tangible or intangible and may include physical, psychological, social or economic harm.

(6) Given the significant impact that AI can have on society and the need to build trust, it is
It is essential that AI and its regulatory framework be developed in accordance with the Union values enshrined in Article 2 of the Treaty on European Union (TEU), the fundamental rights and freedoms enshrined in the Treaties and, in accordance with Article 6 TEU, the Charter. As a prerequisite, AI must be a human-centred technology. Furthermore, it must be a tool for people and ultimately aim to increase human well-being.

(7) Common rules for high-risk AI systems should be established in order to ensure a high and consistent level of protection of public interests with regard to health, safety and fundamental rights. These rules should be consistent with the Charter, should not be discriminatory and should be in line with the Union's commitments on international trade. They should also take into account the European Declaration on Digital Rights and Principles for the Digital Decade and the Ethical Guidelines for Trustworthy AI of the Independent High-Level Expert Group on Artificial Intelligence.

(8) An EU legal framework setting out harmonised AI rules is therefore needed to boost the development, use and adoption of AI in the internal market, while providing a high level of protection of public interests, such as health and safety and the protection of fundamental rights, including democracy, the rule of law and environmental protection, recognised and protected by Union law. To achieve this objective, rules should be laid down for the placing on the market, commissioning and use of certain AI systems, which will ensure the smooth functioning of the internal market and allow such systems to benefit from the principle of free movement of goods and services. Those rules should be clear and robust in protecting fundamental rights, supporting new innovative solutions, enabling a European ecosystem of public and private actors building AI systems in line with Union values and unleashing the potential of digital transformation in all regions of the Union. By establishing such rules, as well as measures in support of innovation with a particular focus on small and medium-sized enterprises (SMEs), including start-ups, this Regulation supports the objective of promoting the European human-centred approach to AI and of being a world leader in the development of safe, trustworthy and ethical AI, as indicated by the European Council [5], and ensures the protection of ethical principles, as specifically requested by the European Parliament [6].

[5] European Council, Extraordinary meeting of the European Council (1-2 October 2020) – Conclusions, EUCO 13/20, 2020, p. 6.

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

(9) Harmonised rules should be established for the placing on the market, putting into service and use of high-risk AI systems in line with Regulation (EC) No 1999/2003.either765/2008 of the European Parliament and of the Council [7], Decision No.either768/2008/EC of the European Parliament and of the Council [8] and Regulation (EU) 2019/1020 of the European Parliament and of the Council [9] (hereinafter 'the new legislative framework'). The harmonised rules set out in this Regulation should apply across all sectors and, in line with the new legislative framework, should be without prejudice to existing Union law, in particular on data protection, consumer protection, fundamental rights, employment, worker protection and product safety, which this Regulation supplements. Consequently, all rights and remedies granted by that Union law to consumers and other persons who may be adversely affected by AI systems, including with regard to the remedy of any damage in accordance with Council Directive 85/374/EEC [10]. Furthermore, in the context of employment and the protection of workers, this Regulation should therefore not affect Union law on social policy or national labour law – in accordance with Union law – relating to employment and working conditions, including health and safety at work and the relationship between employers and employees. This Regulation should also not affect in any way the exercise of fundamental rights recognised in the Member States and at Union level, including the right or freedom to strike or to take other action provided for in the specific industrial relations systems of the Member States and the right to negotiate, conclude and enforce collective agreements or to take collective action in accordance with national law. This Regulation should not affect provisions aimed at improving working conditions in digital platform work set out in a Directive of the European Parliament and of the Council on improving working conditions in digital platform work. Furthermore, this Regulation aims to strengthen the effectiveness of such existing rights and remedies by establishing specific requirements and obligations, including as regards transparency, technical documentation and record keeping of AI systems. Furthermore, the obligations imposed on the various operators involved in the AI value chain under this Regulation should apply without prejudice to national law which, in accordance with Union law, has the effect of limiting the use of certain AI systems where such law falls outside the scope of this Regulation or pursues legitimate public interest objectives other than those pursued by this Regulation. Thus, for example, this Regulation should not affect national labour law or law on the protection of minors, namely persons under the age of 18, which take into account General Comment No 101/2008.either25 (2021) of the United Nations Convention on the Rights of the Child on the rights of the child in relation to the digital environment, to the extent that they are not specific to AI systems and pursue other legitimate objectives of public interest.

(10) The fundamental right to the protection of personal data is guaranteed, in particular, by the Regulations (EU) 2016/679 [11] and (EU) 2018/1725 [12] of the European Parliament and of the Council and Directive (EU) 2016/680 of the European Parliament and of the Council [13]. Furthermore, Directive 2002/58/EC of the European Parliament and of the Council [14] protects privacy and the confidentiality of communications, including by setting out conditions for any storage of personal and non-personal data on, and access from, terminal equipment. Those Union legislative acts form the basis for sustainable and responsible data processing, including where data sets contain a mix of personal and non-personal data. This Regulation is not intended to affect the application of existing Union law governing the processing of personal data, including the roles and powers of independent supervisory authorities competent to monitor compliance with those instruments. It also does not affect the obligations of providers and those responsible for deploying AI systems in their role as data controllers or processors.

[7] Regulation (EC) No.either765/2008 of the European Parliament and of the Council of 9 July 2008 laying down the requirements for accreditation and repealing Regulation (EEC) No.either339/93 (OJ L 218, 13.8.2008, p. 30).

[8] Decision no.either768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products and repealing Council Decision 93/465/EEC (OJ L 218, 13.8.2008, p. 82).

[9] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and conformity of products and amending Directive 2004/42/EC and Regulations (EC) No 1020/2009 and (EC) No 1020/2009 of the European Parliament and of the Council.either765/2008 and (EU) n.either 305/2011 (OJ L 169, 25.6.2019, p. 1).

[10] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for damage caused by defective products (OJ L 210 of 7.8.1985, p. 29).

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[12] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 1725/2018.either45/2001 and Decision No.either1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

[13] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

[14] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

arising from Union or national law on the protection of personal data to the extent that the design, development or use of AI systems involves the processing of personal data. It should also be clarified that data subjects continue to enjoy all the rights and safeguards conferred on them by such Union law, including rights related to fully automated individual decisions, such as profiling. Harmonised rules for the placing on the market, service and use of AI systems established under this Regulation should facilitate the effective implementation and enable the exercise of rights and other remedies of data subjects guaranteed by Union law on the protection of personal data, as well as other fundamental rights.

(11) This Regulation should be interpreted without prejudice to the provisions of Regulation (EU) 2022/2065 of the European Parliament and of the Council [15] relating to the liability of providers of intermediary services.

(12) The concept of an 'AI system' should be clearly defined in this Regulation and closely aligned with the work of international organisations dealing with AI, in order to ensure legal certainty and facilitate international convergence and broad acceptance, while providing the necessary flexibility to accommodate rapid technological developments in this field. Furthermore, the definition should be based on the main characteristics of AI systems that distinguish them from non-AI systems.softwareor traditional, simpler programming approaches, and should not include systems based on rules defined solely by natural persons to automatically execute operations. A key feature of AI systems is their inference capability. Inference capability refers to the process of obtaining output results, such as predictions, content, recommendations, or decisions, that can influence physical and virtual environments, and to the ability of AI systems to deduce models or algorithms, or both, from input information or data. Techniques that enable inference when building an AI system include machine learning strategies that learn from data how to achieve certain goals, and logic- and knowledge-based strategies that infer from encoded knowledge or a symbolic representation of the task to be solved. The inference capability of an AI system goes beyond basic data processing by enabling learning, reasoning, or modeling. The term “machine-based” refers to the fact that AI systems run on machines. The reference to explicit or implicit objectives underlines that AI systems may operate according to explicit defined objectives or implicit objectives. The objectives of the AI system may be different from the intended purpose of the AI system in a specific context. For the purposes of this Regulation, environments should be understood as the contexts in which AI systems operate, while the output results generated by the AI system reflect the different functions performed by AI systems and include predictions, content, recommendations or decisions. AI systems are designed to operate with different levels of autonomy, meaning that they can act with a certain degree of independence from human action and have certain capabilities to operate without human intervention. The adaptive capacity that an AI system could display after deployment refers to self-learning capabilities that allow the system to change while in use. AI systems can be used independently or as components of a product, regardless of whether the system is physically part of the product (embedded) or contributes to the functionality of the product without being part of it (non-embedded).

(13) The concept of ‘deployment controller’ as referred to in this Regulation should be interpreted as any natural or legal person, including any public authority, body, office or agency, using an AI system under its own authority, except where its use is in the context of a personal, non-professional activity. Depending on the type of AI system, the use of the system may affect persons other than the deployer.

(14) The concept of ‘biometric data’ as used in this Regulation should be interpreted in the light of the concept of ‘biometric data’ as defined in point (14) of Article 4 of Regulation (EU) 2016/679, point (18) of Article 3 of Regulation (EU) 2018/1725 and point (13) of Article 3 of Directive (EU) 2016/680. Biometric data may allow for the authentication, identification or categorisation of natural persons and the recognition of the emotions of natural persons.

(15) The concept of "biometric identification" referred to in this Regulation should be defined as the automated recognition of physical, physiological or behavioural characteristics of a human being, such as face, eye movement, body shape, voice, intonation, gait, posture, heart rate, blood pressure, odour or keystroke characteristics, to determine the identity of an individual by comparing his or her biometric data with the biometric data of individuals stored in a reference database, whether or not the individual has given consent. Excluded are AI systems intended for biometric verification, which includes authentication, the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be, as well as the identity of a natural person for the sole purpose of enabling that person to access a service, unlock a device or grant secure access to a premises.

[15] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Regulation) (OJ L 277, 27.10.2022, p. 1).

(16) The concept of ‘biometric categorisation’ as referred to in this Regulation should be defined as the inclusion of natural persons in specific categories on the basis of their biometric data. Such specific categories may relate to aspects such as sex, age, hair colour, eye colour, tattoos, behavioural or personality traits, language, religion, membership of a national minority, sexual or political orientation. This does not include biometric categorisation systems which are a purely incidental characteristic intrinsically linked to another commercial service, meaning that the characteristic cannot, for objective technical reasons, be used without the main service and that the integration of such a characteristic or functionality is not a means of circumventing the applicability of the rules of this Regulation. For example, filters classifying facial or body characteristics used in online marketplaces could constitute such an incidental characteristic as they can only be used in relation to the main service, which is to sell a product by allowing the consumer to preview how it would look on him or her and to assist him or her in making a purchasing decision. Filters used in social networking services that classify facial or body features so that users can add or modify images or videos could also be considered an accessory feature, since such filters cannot be used without the core service of social networking, which is sharing content online.

(17) The concept of a 'remote biometric identification system' as referred to in this Regulation should be functionally defined as an AI system intended to identify natural persons without their active participation, usually remotely, by comparing their biometric data with those in a reference database, regardless of the specific technology, processes or types of biometric data used.
These remote biometric identification systems are typically used to detect multiple individuals or their behaviour simultaneously, in order to significantly simplify the identification of individuals without their active involvement. Excluded are AI systems intended for biometric verification, which includes authentication, the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be, as well as the identity of a natural person for the sole purpose of granting him or her access to a service, unlocking a device or securing access to a premises. This exclusion is justified by the fact that such systems are likely to have a lesser impact on the fundamental rights of natural persons than remote biometric identification systems that can be used to process the biometric data of a large number of individuals without their active involvement. In the case of “real-time” systems, the collection of biometric data, comparison and identification occur instantaneously, almost instantaneously or, in any case, without significant delay. In this regard, there should be no possibility to circumvent the rules laid down in this Regulation in relation to the “real-time” use of the AI systems concerned by creating minimal delays. “Real-time” systems involve the use of “live” or “near-live” materials, such as video recordings, generated by a camera or other device with similar functions. In contrast, in “delayed” systems, biometric data have already been collected and comparison and identification occur with a significant delay. For this purpose, materials such as images or video recordings captured by closed-circuit television cameras or private devices, generated prior to the use of the system in relation to the natural persons concerned, are used.

(18) The concept of ‘emotion recognition system’ as referred to in this Regulation should be defined as an AI system intended to distinguish or infer the emotions or intentions of natural persons from their biometric data. The concept refers to emotions or intentions such as happiness, sadness, indignation, surprise, disgust, embarrassment, excitement, embarrassment, contempt, satisfaction and amusement. It does not include physical states such as pain or fatigue, as for example systems used to detect fatigue in professional drivers or pilots in order to prevent accidents. It also does not include the mere detection of obvious expressions, gestures or movements, unless they are used to distinguish or infer emotions. Such expressions may be basic facial expressions such as a frown or a smile; gestures such as the movement of hands, arms or head; or characteristics of a person’s voice such as a raised voice or a whisper.

(19) For the purposes of this Regulation, the concept of ‘publicly accessible space’ should be understood as referring to any physical space to which an indeterminate number of natural persons may have access, regardless of whether it is privately or publicly owned and regardless of the activity for which the space may be used, whether commercial activities, for example shops, restaurants, cafés; service provision activities, for example banks, professional activities, hospitality; sports activities, for example swimming pools, gyms, stadiums; transport activities, for example bus, metro and railway stations, airports, means of transport; entertainment activities, for example cinemas, theatres, museums, concert halls, conference halls; leisure or other activities, for example public roads and squares, parks, forests, playgrounds. Furthermore, a space should be considered to be publicly accessible if, regardless of possible capacity or security restrictions, access is subject to certain predefined conditions that can be met by an indeterminate number of persons, such as the purchase of a ticket or a transport ticket, prior registration or being of a certain age. On the contrary, a space should not be considered to be publicly accessible if it is accessible only to certain defined natural persons, whether by virtue of Union or national law directly related to public security or by virtue of a clear manifestation of the will of the person exercising authority.

relevant to that space. The actual possibility of access, such as an unlocked door or an open gate, does not in itself make the space publicly accessible if there are indications or circumstances suggesting otherwise, such as signs prohibiting or restricting access. Business and factory premises, as well as offices and workplaces intended for access only by relevant employees and service providers, are not publicly accessible spaces. Prisons and areas where border inspections are carried out should not be included in publicly accessible spaces. Some spaces may include both publicly accessible areas and areas that are not publicly accessible, such as airports or the lobby of a private residential building through which one enters a medical office. Online spaces are not publicly accessible places, as they are not physical spaces. However, whether a space is publicly accessible or not should be determined on a case-by-case basis taking into account the particularities of the specific situation.

(20) In order to obtain the greatest benefits from AI systems, while protecting the rights
In order to protect fundamental human rights, health and safety, and to enable democratic control, AI literacy should provide providers, deployers and affected persons with the necessary concepts to make informed decisions regarding AI systems. Those concepts may vary depending on the relevant context and include an understanding of the correct application of the technical elements during the development phase of the AI system, the measures to be applied during its use, appropriate ways to interpret the output results of the AI system and, for affected persons, the necessary knowledge to understand how decisions taken with the help of AI will have an impact on them. In the context of the application of this Regulation, AI literacy should provide all relevant actors in the AI value chain with the necessary knowledge to ensure proper compliance and correct implementation. Furthermore, the widespread implementation of AI literacy measures and the introduction of appropriate follow-up actions could contribute to improving working conditions and ultimately support the consolidation and innovation path of trustworthy AI in the Union. The European Artificial Intelligence Council ('AI Council') should support the Commission in promoting AI literacy tools, public awareness and understanding of the benefits, risks, safeguards, rights and obligations in relation to the use of AI systems. In cooperation with relevant stakeholders, the Commission and the Member States should facilitate the development of voluntary codes of conduct to promote AI literacy among those involved in the development, operation and use of AI.

(21) In order to ensure a level playing field and the effective protection of individuals' rights and freedoms throughout the Union, the rules set out in this Regulation should apply to providers of AI systems without discrimination, regardless of whether they are established in the Union or in a third country, and to those responsible for the deployment of AI systems established in the Union.

(22) Due to their digital nature, some AI systems should fall within the scope of this Regulation even if they are not placed on the market, put into service or used in the Union. This is the case, for example, where an operator established in the Union enters into a contract with an operator established in a third country for the provision of certain services in relation to an activity to be carried out by an AI system that would be considered high-risk. In such circumstances, the AI system used in a third country by the operator could process data lawfully collected in the Union and transferred from its territory, and provide the contracting operator located in the Union with the output results generated by that AI system as a result of this processing without the AI system in question being placed on the market, put into service or used in the Union.
In order to prevent circumvention of this Regulation and to ensure the effective protection of natural persons located in the Union, this Regulation should also apply to providers and controllers of the deployment of AI systems established in a third country, insofar as the output results generated by such systems are intended for use in the Union. However, in order to take into account existing agreements and special needs for future cooperation with foreign partners with whom information and evidence are exchanged, this Regulation should not apply to public authorities of a third country or to international organisations when acting within the framework of international or cooperation agreements concluded at national or Union level for the purposes of law enforcement and judicial cooperation with the Union or its Member States if the relevant third country or international organisation provides sufficient guarantees with regard to the protection of the fundamental rights and freedoms of individuals. Where appropriate, this may include the activities of entities to which third countries have entrusted specific tasks in support of such law enforcement and judicial cooperation. Such cooperation frameworks or agreements have been established bilaterally between Member States and third countries or between the European Union, Europol and other Union bodies and third countries and international organisations. The authorities competent for the supervision of law enforcement and judicial authorities under this Regulation should assess whether such international cooperation frameworks or agreements include sufficient safeguards with regard to the protection of the fundamental rights and freedoms of individuals. National authorities and Union institutions, bodies, offices and agencies that are recipients of such output and that use it in the Union remain responsible for ensuring that their use of the

information is in line with Union law. When, in the future, such international agreements are revised or new ones are concluded, the contracting parties should make every effort to ensure that such agreements comply with the requirements of this Regulation.

(23) This Regulation should also apply to Union institutions, bodies, offices and agencies when acting as providers or those responsible for the deployment of an AI system.

(24) Where and to the extent that AI systems are placed on the market, put into service or used, with or without modification, for military, defence or national security purposes, they should be excluded from the scope of this Regulation, regardless of the type of entity carrying out those activities, for example, whether it is a public or a private entity. As regards military and defence purposes, such exclusion is justified both by Article 4(2) TEU and by the specificities of the Member States' defence policy and the Union's common defence policy referred to in Title V, Chapter 2 TEU, which are subject to public international law, which is therefore the most appropriate legal framework for the regulation of AI systems in the context of the use of lethal force and other AI systems in the context of military and defence activities. As regards national security purposes, the exclusion is justified both by the fact that national security remains the exclusive responsibility of Member States pursuant to Article 4(2) TEU and by the specific nature and operational needs of national security activities and by the specific national rules applicable to such activities. However, if an AI system developed, placed on the market, put into service or used for military, defence or national security purposes were to be used temporarily or permanently outside these areas for other purposes (for example, for civil or humanitarian purposes, law enforcement or public security), that system would fall within the scope of this Regulation. In such a case, the entity using the AI system for purposes other than military, defence or national security purposes should ensure that the AI system complies with this Regulation, unless the system already does so. AI systems placed on the market or put into service for an excluded purpose,

namely military, defence or national security purposes, and one or more non-excluded purposes, such as civil or law enforcement purposes, fall within the scope of this Regulation and providers of such systems should ensure compliance with this Regulation. In such cases, the fact that an AI system may fall within the scope of this Regulation should not affect the possibility for entities carrying out military, defence and national security activities, regardless of the type of entity carrying out those activities, to use AI systems for military, defence and national security purposes, the use of which is excluded from the scope of this Regulation. An AI system placed on the market for civil or law enforcement purposes that is used, with or without modifications, for military, defence or national security purposes should not fall within the scope of this Regulation, regardless of the type of entity carrying out those activities.

(25) This Regulation should support innovation, respect the freedom of science and not undermine research and development activity. It is therefore necessary to exclude from its scope AI systems and models that are specifically developed and put into service solely for scientific research and development purposes. Furthermore, it is necessary to ensure that this Regulation does not otherwise affect scientific research and development activity on AI systems or models before they are placed on the market or put into service. As regards product-oriented research, testing and development activity on AI systems or models, the provisions of this Regulation should also not apply before such systems and models are put into service or put into service. That exclusion is without prejudice to the obligation to comply with this Regulation when an AI system falling within the scope of this Regulation is placed on the market or put into service as a result of such research and development activity, as well as to the application of provisions on AI sandboxes and real-world testing. Furthermore, without prejudice to the exclusion of AI systems specifically developed and put into service solely for scientific research and development purposes, any other AI system that may be used to carry out any research and development activity should remain subject to the provisions of this Regulation. In any event, any research and development activity should be carried out in accordance with recognised ethical and professional standards for scientific research and applicable Union law.

(26) In order to establish a proportionate and effective set of binding rules for AI systems, a clearly defined risk-based approach is needed, tailoring the type and content of the rules.
the intensity and scope of the risks that the AI systems in question may generate. It is therefore necessary to prohibit certain unacceptable AI practices, to define the requirements to be met by high-risk AI systems and the obligations applicable to relevant operators, and to impose transparency obligations on certain AI systems.

(27) While the risk-based approach is the basis for a proportionate and effective set of binding rules, it is It is important to recall the 2019 Ethical Guidelines for Trustworthy AI, developed by the Independent High-Level Expert Group on AI established by the Commission. In those guidelines, the Independent High-Level Expert Group on AI developed seven non-binding ethical principles for AI that aim to help ensure the trustworthiness and ethical foundation of AI. The seven principles are: human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; social and environmental well-being; and accountability. Without prejudice to the legally binding requirements of this Regulation and any other applicable act of Union law, those guidelines contribute to the design of coherent, trustworthy and human-centred AI, in line with the Charter and the values on which the Union is founded. According to the High-Level Expert Group on AI guidelines, “human agency and oversight” means that AI systems are developed and used as a tool in the service of people, respecting human dignity and personal autonomy, and operating in a way that can be appropriately controlled and monitored by humans. “Technical robustness and safety” means that AI systems are developed and used in a way that is robust to problems and resilient to attempts to alter the use or operation of the AI system to enable unlawful use by third parties and to minimise unintended harm. “Privacy and data management” means that AI systems are developed and used in compliance with privacy and data protection standards, while handling data that meets strict standards in terms of quality and integrity. "Transparency" means that AI systems are developed and used in a way that allows for appropriate traceability and explainability, while making people aware that they are communicating or interacting with an AI system and duly informing those responsible for the deployment about the capabilities and limitations of that AI system and affected individuals about their rights. "Diversity, non-discrimination and fairness" means that AI systems are developed and used in a way that includes diverse actors and promotes equal access, gender equality and cultural diversity, while avoiding discriminatory effects and unfair biases prohibited by Union or national law. "Social and environmental well-being" means that AI systems are developed and used in a sustainable and environmentally friendly manner, as well as for the benefit of all humans,while monitoring and assessing the long-term impacts on people, society and democracy. The application of these principles should, where possible, be reflected in the design and use of AI models. In any case, they should serve as a basis for the development of codes of conduct under this Regulation. All stakeholders, including industry, academia, civil society and standard-setting organisations, are encouraged to take into account, as appropriate, the ethical principles for the development of voluntary standards and best practices.

(28) Beyond the many beneficial uses of AI, it can also be misused and provide powerful new tools for manipulation, exploitation and social control. Such practices are extremely harmful and wrong and must be prohibited as they run counter to the Union's values of respect for human dignity, freedom, equality, democracy and the rule of law and to fundamental rights enshrined in the Charter, such as the right to non-discrimination, data protection and privacy and the rights of the child.

(29) Manipulation techniques enabled by AI can be used to persuade people to engage in undesirable behaviour or to trick them into making decisions in a way that undermines and impairs their autonomy, decision-making and ability to make free choices. They are particularly dangerous and should therefore be prohibited from being placed on the market, put into service or used for the purpose of substantially altering human behaviour, with the likelihood of causing substantial harm, in particular harm with sufficiently significant adverse effects on physical or mental health or financial interests. Such AI systems use subliminal components, such as audio, image or video stimuli that cannot be perceived by humans as such stimuli are beyond human perception, or other manipulative or deceptive techniques that undermine or impair humans' autonomy, decision-making or ability to make free choices in ways that humans are not actually aware of or, when they are aware of such techniques, may still be deceived or unable to control or resist them. This could be facilitated, for example, by brain-machine interfaces or virtual reality, as they allow for a greater degree of control over what stimuli are presented to humans, to the extent that they may substantially alter their behaviour in a way that causes significant harm. In addition, AI systems may also exploit in other ways the vulnerabilities of a person or a specific group of people arising from their age, disability within the meaning of Directive (EU) 2019/882 of the European Parliament and of the Council [16] or from a particular social or economic situation that is likely to increase their vulnerability to exploitation, such as living in extreme poverty or belonging to ethnic or religious minorities. These AI systems may be placed on the market, put into service or used with the aim of, or having the effect of, substantially altering the behaviour of a person, and in a way that causes, or is reasonably likely to cause, substantial harm to that person or another person or group of people, including harm that may accumulate over time and which should therefore be prohibited. It cannot be presumed that there is

[16] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on accessibility requirements for products and services (OJ L 151, 7.6.2019, p. 70).

the intention to alter behaviour if the alteration is the result of factors external to the AI system that are beyond the control of the provider or deployer, namely factors that are not logically foreseeable and therefore cannot be mitigated by the provider or deployer of the AI system. In any case, the provider or deployer need not have the intention to cause substantial harm, provided that such harm results from the manipulative or exploitative practices enabled by AI. The prohibition of such AI practices complements the provisions of Directive 2005/29/EC of the European Parliament and of the Council ([17]), in particular the prohibition, in all circumstances, of unfair commercial practices causing economic or financial harm to consumers, whether established by means of AI systems or otherwise. The prohibition of manipulative and exploitative practices set out in this Regulation should not affect lawful practices in the context of medical treatment, such as psychological treatment of mental illness or physical rehabilitation, where such practices are carried out in accordance with applicable law and medical standards, for example with the express consent of individuals or their legal representatives. Furthermore, common and legitimate commercial practices (for example in the field of advertising) that comply with applicable law should not be considered to be, in themselves, harmful manipulative practices enabled by AI.

(30) Biometric categorization systems based on biometric data of natural persons should be prohibited, such as the face or fingerprints of a natural person, in order to deduce or infer a natural person's political opinions, trade union membership, religious or philosophical beliefs, race, sex life or sexual orientation. That prohibition should not apply to the lawful labelling, filtering or categorisation of biometric data sets acquired in accordance with Union or national law on the basis of biometric data, such as the classification of images based on hair colour or eye colour, which may be used, for example, in the field of law enforcement.

(31) AI systems that enable public or private actors to carry out citizen scoring of natural persons may have discriminatory outcomes and lead to the exclusion of certain groups. They may undermine the right to dignity and non-discrimination and the values of equality and justice. Such AI systems assess or rank natural persons or groups of natural persons on the basis of multiple data points relating to their social behaviour in multiple contexts or on known, inferred or predicted personal or personality characteristics over certain periods of time. The citizen scoring resulting from such AI systems may lead to harmful or unfavourable treatment of certain natural persons or entire groups in social contexts unrelated to the context where the data was originally generated or collected, or to harmful treatment that is disproportionate or unjustified in relation to the severity of their social behaviour. Therefore, AI systems that involve such unacceptable scoring practices and lead to such harmful or unfavourable outcomes should be prohibited. This prohibition should not affect lawful assessment practices of natural persons carried out for a specific purpose in accordance with Union and national law.

(32) The use of AI systems for remote “real-time” biometric identification of natural persons in publicly accessible spaces for law enforcement purposes encroaches particularly severely on the rights and freedoms of the individuals concerned, as it may affect the private lives of a large part of the population, create a feeling of being under constant surveillance and indirectly deter citizens from exercising their freedom of assembly and other fundamental rights. Technical inaccuracies in AI systems intended for remote biometric identification of natural persons may lead to biased results and have discriminatory effects. Such potential biased results and discriminatory effects are particularly relevant with regard to age, ethnicity, race, sex or disability. Furthermore, the immediacy of the consequences and the limited opportunities for additional checks or corrections in connection with the use of systems operating in "real time" increase the risk that they pose to the rights and freedoms of persons affected by or in the context of law enforcement activities.

(33) Accordingly, the use of such systems for the purposes of ensuring compliance with the law should be prohibited. except in narrowly listed and precisely defined situations where their use is strictly necessary to achieve an essential public interest the importance of which outweighs the risks. Such situations include the search for certain victims of a crime, including missing persons; certain threats to the life or physical safety of natural persons or threats of a terrorist attack; and the location or identification of the perpetrators or suspects of the offences listed in an Annex to this Regulation, where such offences are punishable in the Member State concerned by a penalty or a fine.

[17] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 1017/2005.either2006/2004 of the European Parliament and of the Council (‘Unfair Commercial Practices Directive’) (OJ L 149, 11.6.2005, p. 22).

a custodial sentence or a custodial measure of a maximum duration of at least four years, as defined in the law of that Member State. Setting such a threshold for a custodial sentence or a custodial measure under national law helps to ensure that the offence is serious enough to justify the use of remote "real-time" biometric identification systems. Furthermore, the list of offences provided for in an annex to this Regulation is based on the thirty-two offences listed in Council Framework Decision 2002/584/JHA [18], although it should be noted that in practice some are likely to be more relevant than others in the sense that it is foreseeable that the use of remote “real-time” biometric identification could be necessary and proportionate to very different degrees in order to locate or identify the perpetrators or suspects of the various offences listed, and that there are likely to be differences in the severity, likelihood and magnitude of the harm or potential negative consequences. An imminent threat to the life or physical security of natural persons could also arise from a serious disruption of critical infrastructure, as defined in point 4 of Article 2 of Directive (EU) 2022/2557 of the European Parliament and of the Council [19], where the disruption or destruction of such critical infrastructure would pose an imminent threat to the life or physical security of a person, including by seriously undermining the supply of essential products to the population or the exercise of the essential function of the State. In addition, this Regulation should preserve the ability of law enforcement, border control, immigration or asylum authorities to carry out identity checks in the presence of the person concerned, in accordance with the conditions laid down in Union and national law for such checks. In particular, law enforcement, border control, immigration or asylum authorities should be able to use information systems, in accordance with Union or national law, to identify persons who, during an identity check, refuse to be identified or are unable to declare or prove their identity, without this Regulation requiring prior authorisation to be obtained. This may be, for example, a person involved in a crime who does not want to reveal his or her identity to law enforcement authorities, or who is unable to do so due to an accident or a medical condition.

(34) In order to ensure that such systems are used in a responsible and proportionate manner, it is also important to provide that, in those situations listed in a limited manner and precisely defined, certain elements are taken into account, in particular as regards the nature of the situation giving rise to the request,
the consequences that their use may have on the rights and freedoms of all persons concerned, and the safeguards and conditions accompanying their use. Furthermore, the use of remote "real-time" biometric identification systems in publicly accessible spaces for enforcement purposes should be carried out only to confirm the identity of the person who is the specific target and should be limited to what is strictly necessary as regards the time period, as well as the geographical and personal scope, taking into account, in particular, evidence or indications concerning threats, victims or perpetrators. The use of the remote real-time biometric identification system in publicly accessible spaces should only be authorised if the relevant law enforcement authority has carried out a fundamental rights impact assessment and, unless otherwise provided for in this Regulation, has registered the system in the database established by this Regulation. The database of reference persons should be appropriate for each scenario of use in each of the above-mentioned situations.

(35) Any use of a remote “real-time” biometric identification system in publicly accessible spaces for the purposes of law enforcement must have been expressly and specifically authorised by a judicial authority or an independent administrative authority of a Member State and whose decision is binding. In principle, such authorisation must be obtained before the AI system is used for the purpose of identifying one or more persons. Exceptions to that rule should be permitted in situations duly justified on grounds of urgency, namely where the need to use the systems in question is so compelling that it is effectively and objectively impossible to obtain authorisation before starting to use the AI system. In such urgent situations, the use should be limited to the minimum necessary and should satisfy the appropriate safeguards and conditions, as provided for by national law and as appropriate in each specific case of urgent use by the enforcement authority itself. Furthermore, in such situations, law enforcement authorities should request such authorisation and state the reasons why they have not been able to do so before, without undue delay and at the latest within 24 hours. If such authorisation is refused, the use of real-time biometric identification systems linked to the authorisation should be discontinued with immediate effect and all data related to such use should be discarded and deleted. Such data includes input data directly acquired by an AI system during the use of such a system, as well as results and output information of the use linked to such authorisation. It should not include input information lawfully acquired pursuant to another act of national or Union law. In any event, no decision producing effects should be adopted.

[18] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1).

[19] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333, 27.12.2022, p. 164).

adverse legal consequences for a person solely on the basis of the output results of the remote biometric identification system.

(36) In order to carry out their tasks in accordance with the requirements set out in this Regulation as well as in national rules, the relevant market surveillance authority and the national data protection authority should be notified of each use of the real-time biometric identification system. Market surveillance authorities and national data protection authorities that have received a notification should submit to the Commission an annual report on the use of real-time biometric identification systems.

(37) On the other hand, it is appropriate to provide, within the comprehensive framework established by this Regulation, that such use in the The use of such equipment on the territory of a Member State under this Regulation should only be possible where and to the extent that the Member State concerned has decided to provide expressly for the possibility of authorising such use in the detailed rules of its national law. Accordingly, Member States remain free under this Regulation not to provide for such use at all or to provide such use only in relation to some of the purposes which may justify authorised use under this Regulation. Such national rules must be notified to the Commission within 30 days of their adoption.

(38) The use of AI systems for remote real-time biometric identification of natural persons in public spaces for law enforcement purposes necessarily involves the processing of biometric data. The rules of this Regulation prohibiting, with certain exceptions, such use, based on Article 16 TFEU, should apply aslex specialiswith regard to the rules on the processing of biometric data set out in Article 10 of Directive (EU) 2016/680, thereby comprehensively regulating such use and processing of the relevant biometric data. Such use and processing should therefore be possible only to the extent that they are compatible with the framework established by this Regulation, with no scope, outside that framework, for competent authorities, when acting for enforcement purposes, to use such systems and process such data in the cases provided for in Article 10 of Directive (EU) 2016/680. In that regard, this Regulation is not intended to provide the legal basis for the processing of personal data pursuant to Article 8 of Directive (EU) 2016/680. However, the use of remote real-time biometric identification systems in publicly accessible spaces for purposes other than enforcement, including by competent authorities, should not be subject to the specific framework set out in this Regulation as regards the use of such systems for enforcement purposes. Consequently, their use for purposes other than enforcement should not be subject to the requirement to obtain an authorisation provided for in this Regulation or to the applicable implementing rules of national law that may give effect to such an authorisation.

(39) Any processing of biometric data and other personal data associated with the use of AI systems for biometric identification, except for processing associated with the use of remote real-time biometric identification systems in publicly accessible spaces for enforcement purposes governed by this Regulation, must continue to comply with all the requirements arising from Article 10 of Directive (EU) 2016/680. Article 9(1) of Regulation (EU) 2016/679 and Article 10(1) of Regulation (EU) 2018/1725 prohibit the processing of biometric data for purposes other than enforcement, subject to the limited exceptions provided for in those Articles. In the application of Article 9(1) of Regulation (EU) 2016/679, the use of remote biometric identification for purposes other than enforcement has already been the subject of prohibition decisions by national data protection authorities.

(40) Pursuant to Article 6Bisof Protocol No.either21 on the Position of the United Kingdom and Ireland in respect of the Area of Freedom, Security and Justice, annexed to the TEU and to the TFEU, the rules laid down in point (g) of the first subparagraph of Article 5(1), insofar as it applies to the use of biometric categorisation systems for activities in the field of police cooperation and judicial cooperation in criminal matters, point (d) of the first subparagraph of Article 5(1), insofar as it applies to the use of AI systems falling within the scope of that Article, point (h) of the first subparagraph of Article 5(1), paragraphs 2 to 6, and Article 26(10) of this Regulation, adopted on the basis of Article 16 TFEU and relating to the processing of personal data by Member States in the exercise of activities falling within the scope of Part Three, Title V, Chapters 4 or 5 of that Treaty, shall be binding on Ireland only to the extent that rules on this Regulation are binding on Ireland. of the Union regulating forms of judicial cooperation in criminal matters and police cooperation, within the framework of which the provisions established on the basis of Article 16 TFEU must be respected.

(41) In accordance with the provisions of Articles 2 and 2Bisof Protocol No.either22 on the Position of Denmark, annex to the TEU and to the TFEU, the rules laid down in point (g) of the first subparagraph of Article 5(1), insofar as it applies to the use of biometric categorisation systems for activities in the field of police cooperation and judicial cooperation in criminal matters, point (d) of the first subparagraph of Article 5(1), insofar as they apply to the use of AI systems falling within the scope of that Article, Article 5,

Paragraph 1, first subparagraph, point (h), paragraphs 2 to 6 and Article 26(10) of this Regulation, adopted on the basis of Article 16 TFEU and which relate to the processing of personal data by Member States in the course of activities falling within the scope of Part Three, Title V, Chapter 4 or 5 of that Treaty, shall not be binding on or applicable to Denmark.

(42) In line with the presumption of innocence, natural persons in the Union should always be judged on the basis of their actual behaviour. Natural persons should never be judged on the basis of behaviour predicted by an AI based solely on their profiling, personality traits or characteristics, such as nationality, place of birth, place of residence, number of children, level of indebtedness or type of vehicle, without a human assessment and without a reasonable suspicion, based on verifiable objective facts, that that person is involved in criminal activity. Therefore, risk assessments carried out in respect of natural persons in order to assess the likelihood that they will commit a crime or to predict the commission of an actual or potential crime based solely on the profiling of those natural persons or the assessment of their personality traits and characteristics should be prohibited. In any case, this prohibition does not refer to or concern risk analyses that are not based on the profiling of individuals or on the personality traits and characteristics of individuals, such as AI systems that use risk analysis to assess the likelihood of financial fraud by companies on the basis of suspicious transactions or risk analysis tools to predict the likelihood of detection of narcotics and illicit goods by customs authorities, for example based on known trafficking routes.

(43) The placing on the market, putting into service for that purpose or using AI systems that create or expand facial recognition databases by non-selectively extracting facial images from the internet or CCTV images should be prohibited, as such practices exacerbate feelings of mass surveillance and may lead to serious violations of fundamental rights, including the right to privacy.

(44) There are serious concerns regarding the scientific basis of AI systems that seek to detect or infer emotions, especially since the expression of emotions varies considerably between cultures and situations, and even within the same person. Some of the main shortcomings of these systems are limited reliability, lack of specificity and limited generalizability. Consequently, AI systems that detect or infer emotions or intentions of natural persons from their biometric data may have discriminatory outcomes and may encroach on the rights and freedoms of the affected individuals. Considering the imbalance of power in the workplace or educational context, coupled with the intrusive nature of these systems, such systems could lead to harmful or unfavourable treatment of certain natural persons or entire groups. Therefore, the placing on the market, commissioning and use of AI systems intended to be used to detect the emotional state of individuals in workplace and educational situations should be prohibited. Such a ban should not apply to AI systems placed on the market strictly for medical or security purposes, such as systems intended for therapeutic use.

(45) This Regulation should not affect practices prohibited by Union law, including Union data protection law, non-discrimination law, consumer protection law and competition law.

(46) The placing on the Union market, putting into service or use of high-risk AI systems should be subject to compliance by you with certain mandatory requirements, which should ensure that high-risk AI systems available in the Union or the output of which is used in the Union do not pose unacceptable risks to important public interests of the Union, recognised and protected by Union law. On the basis of the new legislative framework, as clarified in the Commission Communication entitled "Blue Guide on the implementation of EU product rules, 2022" [20], the general rule is that more than one legal act of Union harmonisation legislation, such as Regulations (EU) 2017/745 [21] and (EU) 2017/746 [22] of the European Parliament and of the Council or Directive 2006/42/EC of the European Parliament and of the Council [23] may be applied to a product, since placing on the market or putting into service can only take place when the product complies with all applicable Union harmonisation legislation. In order to

[20] OJ C 247 of 29.6.2022, p. 1.

[21] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 1018/2009 and Regulation (EC) No 1018/2009.either178/2002 and Regulation (EC) No.either1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1).

[22] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on diagnostic medical devicesin vitroand repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).

[23] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery and amending Directive 95/16/EC (OJ L 157, 9.6.2006, p. 24).

In order to ensure consistency and avoid unnecessary administrative burdens or costs, suppliers of a product containing one or more high-risk AI systems, to which the requirements of this Regulation and of Union harmonisation legislation listed in an Annex to this Regulation apply, should be flexible with regard to operational decisions regarding how to ensure the compliance of a product containing one or more AI systems with all applicable requirements of Union harmonisation legislation in an optimal manner. The classification of an AI system as 'high-risk' should be limited to those AI systems that have a significant adverse effect on the health, safety and fundamental rights of persons in the Union, and such limitation should minimise any potential restrictions on international trade.

(47) AI systems can have an adverse impact on human health and safety, in particular when they operate as safety components of products. In line with the objectives of Union harmonisation legislation to facilitate the free movement of products in the internal market and to ensure that only safe and compliant products reach the market, it is important to properly prevent and mitigate safety risks that a product as a whole may pose due to its digital components, which may include AI systems. For example, increasingly autonomous robots used in factories or for personal care and assistance purposes must be able to operate and perform their functions safely in complex environments. Similarly, in the healthcare sector, where there may be particularly significant impacts on life and health, increasingly sophisticated diagnostic and human decision support systems must be reliable and accurate.

(48) The magnitude of the adverse consequences of an AI system for fundamental rights protected by the Charter is particularly important when classifying an AI system as high risk. These rights include the right to human dignity, respect for private and family life, protection of personal data, freedom of expression and information, freedom of assembly and association, the right to non-discrimination, the right to education, consumer protection, workers' rights, rights of persons with disabilities, equality between men and women, intellectual property rights,
the right to an effective remedy and to a fair trial, the rights of defence and the presumption of innocence, and the right to good administration. In addition to these rights, it is worth highlighting the fact that children have specific rights enshrined in article 24 of the Charter and in the United Nations Convention on the Rights of the Child, which are further developed in general comment No.either25 of the UN Convention on the Rights of the Child on the rights of children in relation to the digital environment. Both instruments require that the vulnerabilities of children be taken into account and that they be provided with the protection and assistance necessary for their well-being. When assessing the seriousness of the harm that an AI system may cause, including with regard to human health and safety, the fundamental right to a high level of environmental protection enshrined in the Charter and implemented in Union policies should also be taken into account.

(49) In relation to high-risk AI systems that are security components of products or systems, or that are themselves products or systems falling within the scope of Regulation (EC) No.either300/2008 of the European Parliament and of the Council [24], Regulation (EU) No.either167/2013 of the European Parliament and of the Council [25], Regulation (EU) No.either168/2013 of the European Parliament and of the Council [26], Directive 2014/90/EU of the European Parliament and of the Council [27], Directive (EU) 2016/797 of the European Parliament and of the Council [28], Regulation (EU) 2018/858 of the European Parliament and of the Council [29], Regulation (EU) 2018/1139 of the European Parliament and

[24] Regulation (EC) No.either300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules on civil aviation security and repealing Regulation (EC) No 300/2008.either2320/2002 (OJ L 97, 9.4.2008, p. 72).

[25] Regulation (EU) No.either167/2013 of the European Parliament and of the Council of 5 February 2013 on type-approval of agricultural or forestry vehicles and the market surveillance of such vehicles (OJ L 60, 2.3.2013, p. 1).

[26] Regulation (EU) No.either168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval of two- or three-wheeled vehicles and quadricycles and the market surveillance of such vehicles (OJ L 60, 2.3.2013, p. 52).

[27] Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC (OJ L 257, 28.8.2014, p. 146).

[28] Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on interoperability of the railway system within the European Union (OJ L 138, 26.5.2016, p. 44).

[29] Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on approval and market surveillance of motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 1189/2008 and (EC) No 1189/2008 and repealing ...either715/2007 and (EC) No.either595/2009 and repealing Directive 2007/46/EC (OJ L 151, 14.6.2018, p. 1).

of the Council [30], and Regulation (EU) 2019/2144 of the European Parliament and of the Council [31], it is appropriate to amend those acts to ensure that, when adopting relevant delegated or implementing acts based on them, the Commission takes into account the mandatory requirements for high-risk AI systems provided for in this Regulation, taking into account the technical and regulatory specificities of the different sectors and without interfering with existing governance, conformity assessment and enforcement mechanisms and authorities set out in those acts.

(50) For AI systems that are safety components of products, or are products in themselves, and fall within the scope of certain Union harmonisation legislation listed in an annex to this Regulation, it is appropriate to classify them as high-risk under this Regulation if the product concerned is subject to a conformity assessment procedure with a third-party conformity assessment body in accordance with those Union harmonisation legislation. Those products are, in particular, machines, toys, lifts, equipment and protection systems for use in potentially explosive atmospheres, radio equipment, pressure equipment, recreational boat equipment, cable transport installations, appliances burning gaseous fuels, medical devices, diagnostic medical devices.in vitro,automotive and aviation.

(51) The fact that an AI system is classified as high-risk under this Regulation does not necessarily mean that the product of which it is a safety component, or the AI system itself as a product, is considered to be 'high-risk' according to the criteria set out in the relevant Union harmonisation legislation that applies to the product. This is the case, in particular, for Regulations (EU) 2017/745 and (EU) 2017/746, which provide for third-party conformity assessment of medium- and high-risk products.

(52) As regards stand-alone AI systems, namely high-risk AI systems that are not safety components of products, or that are products in themselves, they should be classified as high-risk if, in the light of their intended purpose, they present a high risk of harm to the health and safety or fundamental rights of persons, taking into account both the severity of the potential harm and the likelihood of harm occurring, and are used in several predefined areas specified in this Regulation. The same methodology and criteria provided for in the possible future amendment of the list of high-risk AI systems are used to identify such systems, which the Commission should be empowered to adopt, by means of delegated acts, in order to take into account the rapid pace of technological development as well as possible changes in the use of AI systems.

(53) It is also important to clarify that there may be specific cases where AI systems covered by predefined areas specified in this Regulation do not pose a significant risk of harming the legal interests covered by those areas, given that they do not substantially influence decision-making or do not substantially harm such interests. For the purposes of this Regulation, an AI system that does not substantially influence the outcome of decision-making should be understood as an AI system that does not affect the substance, and therefore the outcome, of decision-making, whether human or automated. An AI system that does not substantially influence the outcome of decision-making could include situations where one or more of the following conditions are met. The first of those conditions should be that the AI system is intended to perform a delimited procedural task, such as an AI system that transforms unstructured data into structured data, an AI system that categorises incoming documents or an AI system that is used to detect duplicates across a large number of applications. The nature of those tasks is so restricted and limited that they present only limited risks that are not increased by the use of an AI system in a context that an annex to this Regulation specifies as a high-risk use. The second condition should be that the task performed by the AI system is intended to improve the outcome of an activity

[30] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 1139/2018 and (EC) No 1139/2018 ...either 2111/2005, (EC) No.either1008/2008, (EU) n.either996/2010 and (EU) n.either376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council and Regulations (EC) No.either552/2004 and (EC) No.either216/2008 of the European Parliament and of the Council and Regulation (EEC) No.either3922/91 of the Council (OJ L 212, 22.8.2018, p. 1).

[31] Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, with regard to their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 1899/2002 and (EC) No 1899/2002.either78/2009, (EC) No.either79/2009 and (EC) No.either661/2009 of the European Parliament and of the Council and Regulations (EC) No.either631/2009, (EU) n.either406/2010, (EU) n.either672/2010, (EU) n.either1003/2010, (EU) n.either1005/2010, (EU) n.either1008/2010, (EU) n.either1009/2010, (EU) n.either19/2011, (EU) n.either109/2011, (EU) n.either458/2011, (EU) n.either65/2012, (EU) n.either130/2012, (EU) n.either347/2012, (EU) n.either351/2012, (EU) n.either1230/2012 and (EU) 2015/166 of the Commission (OJ L 325, 16.12.2019, p 1).

A third condition should be that the AI system is intended to detect patterns of decision-making or deviations from previous decision-making patterns. The risk would be lower because the AI system is used after a human assessment has been made and is not intended to replace or influence it without an appropriate review by a human. For example, such AI systems include those that can be used to check the effectiveness of the AI system, and that the AI system is intended to detect a prior human assessment ...a posteriori whether a teacher may have deviated from his or her determined marking pattern, in order to draw attention to possible inconsistencies or anomalies. The fourth condition should be that the AI system is intended to perform a task that is only preparatory for an assessment relevant for the purposes of the AI systems listed in the Annex to this Regulation, with the result that the potential impact of the output results of the system would be very low in terms of posing a risk for the subsequent assessment. This condition includes, inter alia, intelligent solutions for file management, including diverse functions such as indexing, searching, text and speech processing or linking data to other data sources, or AI systems used for the translation of the initial documents. In any case, AI systems used in high-risk cases listed in an Annex to this Regulation should be considered to present a significant risk of undermining health and safety or fundamental rights if the AI system involves profiling within the meaning of point (4) of Article 4 of Regulation (EU) 2016/679, point (4) of Article 3 of Directive (EU) 2016/680 or point (5) of Article 3 of Regulation (EU) 2018/1725. In order to ensure traceability and transparency, suppliers who, based on the above conditions, consider that an AI system is not high-risk, should prepare assessment documentation prior to the placing on the market or entry into service of that AI system and provide it to the competent national authorities upon request. Those suppliers should be obliged to register the system in the EU database established under this Regulation. In order to provide additional guidance on the practical application of the conditions under which AI systems listed in an Annex to this Regulation are not, on an exceptional basis, considered to be high-risk, the Commission should, after consulting the AI Council, provide guidelines specifying such practical application, supplemented by an exhaustive list of practical examples of high-risk and non-high-risk use cases of AI systems.

(54) Since biometric data constitute a category of sensitive personal data, several critical use cases of biometric systems should be classified as high-risk, insofar as their use is permitted under relevant Union and national law. Technical inaccuracies in AI systems intended for remote biometric identification of natural persons may lead to biased results and have discriminatory effects. The risk of such biased results and discriminatory effects is particularly relevant with regard to age, ethnicity, race, sex or disability. Therefore, remote biometric identification systems should be classified as high-risk due to the risks they entail. Excluded from such classification are AI systems intended for biometric verification, including authentication, the sole purpose of which is to confirm that a specific natural person is who that person claims to be, as well as to confirm the identity of a natural person for the sole purpose of granting that person access to a service, unlocking a device or secure access to a premises. Furthermore, AI systems intended to be used for biometric categorisation according to sensitive attributes or characteristics protected pursuant to Article 9(1) of Regulation (EU) 2016/679 on the basis of biometric data, insofar as they are not prohibited under this Regulation, as well as emotion recognition systems that are not prohibited under this Regulation, should be classified as high-risk. Biometric systems intended to be used exclusively for the purposes of enabling cybersecurity and personal data protection measures should not be considered as high-risk AI systems.

(55) As regards the management and operation of critical infrastructure, AI systems intended to be used as security components in the management and operation of critical digital infrastructure listed in point 8 of Annex to Directive (EU) 2022/2557; road traffic and the supply of water, gas, heat and electricity should be classified as high-risk, since a failure or malfunction of these components may endanger the life and health of people on a large scale and significantly disrupt the normal development of social and economic activities. Security components of critical infrastructure, such as critical digital infrastructure, are systems used to directly protect the physical integrity of critical infrastructure or the health and safety of people and property, but which are not necessary for the operation of the system. The failure or defect of

The operation of these components could directly lead to risks to the physical integrity of critical infrastructures and, therefore, to risks to the health and safety of people and property. Components intended to be used exclusively for cybersecurity purposes should not be considered as security components. Security components of such critical infrastructures include water pressure control systems or fire alarm control systems in cloud computing centres.

(56) The deployment of AI systems in education is important to foster high-quality digital education and training and to enable all students and teachers to acquire and share the necessary digital skills and competences, including media literacy and critical thinking, to actively participate in the economy, society and democratic processes. However, AI systems used in education or vocational training, and in particular those that determine access or admission, allocate individuals between different educational and vocational training institutions or programmes at all levels, assess individuals’ learning outcomes, assess the appropriate level of education of an individual and substantially influence the level of education and training that individuals will receive or be able to access, or monitor and detect prohibited behaviour of students during tests, should be classified as high risk, as they may decide an individual’s educational and professional path and, consequently, may affect their ability to secure a livelihood. When not designed and used correctly, these systems can be particularly intrusive and violate the right to education and training, and the right not to be discriminated against, as well as perpetuating historical patterns of discrimination, for example against women, certain age groups, people with disabilities or people of a certain racial or ethnic origin or with a certain sexual orientation.

(57) AI systems used in the fields of employment, workforce management and access to self-employment, in particular for recruitment and selection of staff, for decision-making affecting the terms and conditions of employment relationships, promotion and termination of contractual employment relationships, for the assignment of tasks on the basis of individual behaviour or personal traits or characteristics and for monitoring or evaluating individuals within contractual employment relationships, should also be classified as high-risk, since they may significantly affect the future employment prospects, livelihood of such individuals and workers' rights. Contractual employment relationships should meaningfully include employees and persons providing services via platforms, as outlined in the Commission's 2021 Work Programme. Such systems may perpetuate historical patterns of discrimination, for example against women, certain age groups, persons with disabilities or persons of particular racial or ethnic origins or with a particular sexual orientation, throughout the recruitment process and in the assessment, promotion or retention of persons in contractual employment relationships. AI systems used to monitor the performance and behaviour of such persons may also undermine their fundamental rights to the protection of personal data and privacy.

(58) Access to and enjoyment of certain essential public and private services and benefits necessary for individuals to participate fully in society or improve their standard of living is another area where particular attention should be paid to the use of AI systems. In particular, natural persons who request or receive from public authorities essential public assistance benefits and services, namely health care services, social security benefits, social services ensuring protection in cases such as maternity, illness, industrial accidents, dependency or old age and loss of employment, social assistance and housing assistance, are often dependent on such benefits and services and are generally in a vulnerable position vis-à-vis the responsible authorities. The use of AI systems to decide whether authorities should grant, deny, reduce or revoke such benefits and services or claim their repayment, including, for example, deciding whether beneficiaries are legitimately entitled to such benefits and services, could have a significant impact on individuals' livelihoods and violate their fundamental rights, such as the right to social protection, non-discrimination, human dignity or effective judicial protection, and should therefore be classified as high-risk. However, this Regulation should not hinder the development and use of innovative approaches in government, which could benefit from increased use of compliant and secure AI systems, provided that such systems do not pose a high risk to legal and natural persons. In addition, AI systems used to assess the credit rating or creditworthiness of natural persons, as they decide whether such persons can access financial resources or essential services such as housing, electricity and telecommunications services, should be classified as high-risk. AI systems used for such purposes may discriminate against certain individuals or groups and perpetuate historical patterns of discrimination, such as on the basis of racial or ethnic origin, gender, disability, age or sexual orientation, or give rise to new forms of discrimination. However, AI systems provided for by Union law for the detection of fraud in the supply of financial services and, for prudential purposes, for calculating capital requirements for credit institutions and insurance undertakings should not be considered high-risk under this Regulation. In addition,
AI systems intended to be used for risk assessment and pricing in relation to

11. ...

(59) Given their role and responsibility, actions by law enforcement authorities involving certain uses of AI systems are characterised by a significant imbalance of power and may lead to the surveillance, arrest or deprivation of liberty of a natural person, as well as have other negative effects on fundamental rights enshrined in the Charter. In particular, if the AI system is not trained with good quality data, does not meet appropriate requirements in terms of performance, accuracy or robustness, or is not properly designed and tested before being placed on the market or put into service, it may target individuals in a discriminatory, incorrect or unfair manner. Furthermore, it could impede the exercise of important fundamental procedural rights, such as the right to an effective remedy and to a fair trial, as well as the right to a defence and the presumption of innocence, in particular where such AI systems are not sufficiently transparent, explainable or well documented. Therefore, to the extent that their use is permitted under relevant Union and national law, it is appropriate to classify as high-risk a number of AI systems intended to be used for enforcement purposes where their accuracy, reliability and transparency are particularly important to avoid adverse consequences, maintain public trust and ensure accountability and effective remedies.
In view of the nature of the activities and the associated risks, such high-risk AI systems should include, in particular, AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices or agencies in support of law enforcement authorities, to assess the risk of a natural person becoming a victim of crime, such as polygraph tests and other similar tools, to assess the reliability of evidence during the investigation or prosecution of criminal offences and, to the extent not prohibited under this Regulation, to assess the risk of a natural person committing a criminal offence or reoffending, not only on the basis of profiling of natural persons or the assessment of personality traits and characteristics or past criminal behaviour of natural persons or groups of persons, or for profiling during the detection, investigation or prosecution of criminal offences. AI systems specifically intended for use in administrative processes by tax and customs authorities and financial intelligence units performing administrative tasks of information analysis in accordance with Union anti-money laundering law should not be classified as high-risk AI systems used by law enforcement authorities for the purpose of preventing, detecting, investigating and prosecuting crimes. The use of AI tools by law enforcement authorities and other relevant authorities should not become a factor of inequality or exclusion. The impact of the use of AI tools on the rights of defence of suspects should not be ignored, in particular the difficulty in obtaining meaningful information on the functioning of such systems and the consequent difficulty in challenging their results in court, in particular by natural persons under investigation.

(60) AI systems used in migration, asylum and border control management affect individuals who are often in a particularly vulnerable situation and who are dependent on the outcome of the actions of the competent public authorities. For this reason, it is of utmost importance that AI systems used in these contexts are accurate, non-discriminatory and transparent, in order to ensure that the fundamental rights of the individuals concerned are respected, and in particular their right to free movement, non-discrimination, personal privacy and protection of personal data, international protection and good administration. Therefore, it is appropriate to classify as high-risk, insofar as their use is permitted under Union and national law, those AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies carrying out tasks in the field of migration, asylum and border control management, such as polygraphs and similar tools, to assess certain risks posed by natural persons entering the territory of a Member State or applying for a visa or asylum, to assist the competent public authorities in the examination, including the related assessment of the reliability of evidence, of applications for asylum, visas and residence permits as well as related claims in relation to the objective of determining whether applicant natural persons meet the requirements for their application to be granted, for the purposes of detecting, recognising or identifying natural persons in the context of migration, asylum and border control management, with the exception of the verification of travel documents. AI systems in the field of migration, asylum and border control management subject to this Regulation should comply with the relevant procedural requirements set out in Regulation (EC) No 1099/2008.$_{\text{either}}$810/2009 of the European Parliament and of the

Advice [32], Directive 2013/32/EU of the European Parliament and of the Council [33] and other relevant Union law. The use of AI systems in migration, asylum and border control management should under no circumstances be used by Member States or the Union institutions, bodies, offices or agencies as a means of circumventing their international obligations under the United Nations Convention relating to the Status of Refugees, done at Geneva on 28 July 1951, as amended by the Protocol of 31 January 1967. It should also not be used in any way to infringe the principle of non-refoulement, nor to deny safe and effective legal avenues of access to the territory of the Union, including the right to international protection.

(61) Certain AI systems intended for the administration of justice and democratic processes should be classified as high-risk, given that they may have potentially significant effects on democracy, the rule of law, individual freedoms and the right to an effective remedy and to a fair trial. In particular, in order to address the risk of potential bias, error and opacity, AI systems intended to be used by or on behalf of a judicial authority to assist judicial authorities in investigating and interpreting facts and the law and in applying the law to specific facts should be classified as high-risk. AI systems intended to be used by alternative dispute resolution bodies for such purposes, where the outcomes of alternative dispute resolution procedures have legal effects for the parties, should also be considered high-risk. The use of AI tools may support the decision-making power of judges or judicial independence, but should not replace them: final decision-making should remain a human activity. However, the classification of AI systems as high risk should not be extended to AI systems intended for purely accessory administrative activities that do not affect the administration of justice itself in specific cases, such as the anonymisation or pseudonymisation of judicial decisions, documents or data, communication between staff members or administrative tasks.

(62) Without prejudice to the rules provided for in Regulation (EU) 2024/900 of the European Parliament and of the Council [34], and in order to address the risks of undue external interference with the right to vote enshrined in Article 39 of the Charter and of adverse effects on democracy and the rule of law, AI systems intended to be used to influence the outcome of an election or a referendum, or the electoral behaviour of natural persons when exercising their vote in elections or referendums, should be classified as high-risk AI systems, with the exception of AI systems to whose output natural persons are not directly exposed, such as tools used to organize, optimize and structure political campaigns from an administrative and logistical point of view.

(63) The fact that an AI system is classified as a high-risk AI system under this Regulation should not be interpreted as indicating that its use is lawful under other acts of Union law or national law compatible with Union law, for example on the protection of personal data or the use of polygraphs and similar tools or other systems to detect the emotional state of natural persons. Any such use should continue to be carried out exclusively in line with the relevant requirements arising from the Charter and applicable acts of secondary Union law and national law. This Regulation should not be understood as constituting a legal basis for the processing of personal data, including special categories of personal data, where applicable, unless this Regulation specifically provides otherwise.

(64) In order to mitigate the risks posed by high-risk AI systems placed on the market or put into service, and to ensure a high level of trustworthiness, mandatory requirements should apply to high-risk AI systems, taking into account the intended purpose and context of use of the AI system and in line with the risk management system to be established by the provider. Measures taken by providers to comply with the mandatory requirements of this Regulation should take into account the generally recognised state of the art in AI, be proportionate and effective in achieving the objectives of this Regulation. Based on the new legislative framework, as clarified in the Commission Communication entitled “Blue Guide on the implementation of EU product rules, 2022”, the general rule is that more than one legal act of Union harmonisation legislation may apply to a product, as placing on the market or putting into service can only take place when the product complies with all applicable Union harmonisation legislation. The hazards of AI systems covered by the requirements of this Regulation relate to different aspects than those covered by existing Union harmonisation legislation and therefore the requirements of this Regulation would complement the existing body of Union harmonisation legislation. For example, machines or medical devices incorporating an AI system may present risks that are not addressed by existing Union harmonisation legislation.

[32] Regulation (EC) No.$_{\text{either}}$810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) (OJ L 243, 15.9.2009, p. 1).

[33] Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (OJ L 180, 29.6.2013, p. 60).

[34] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on transparency and targeting in political advertising (OJ L, 2024/900, 20.3.2024, ELI: http://data.europa.eu/eli/reg/2024/900/oj).

essential health and safety requirements set out in the relevant Union harmonised legislation, as that sectoral legislation does not address the specific risks of AI systems. This requires simultaneous and complementary application of several legislative acts. In order to ensure consistency and to avoid unnecessary administrative burden and unnecessary costs, suppliers of a product containing one or more high-risk AI systems, to which the requirements of this Regulation and of Union harmonisation legislative acts based on the new legislative framework and listed in an annex to this Regulation apply, should be flexible with regard to operational decisions concerning how to ensure the compliance of a product containing one or more AI systems with all applicable requirements of Union harmonised legislation in an optimal manner. Such flexibility could mean, for example, the supplier's decision to integrate part of the necessary testing and reporting processes, as well as the information and documentation required under this Regulation, into the already existing documentation and procedures required under existing Union harmonisation legislative acts based on the new legislative framework and listed in an annex to this Regulation. This should not in any way undermine the supplier's obligation to comply with all applicable requirements.

(65) The risk management system should consist of a continuous iterative process that is planned and executed throughout the lifecycle of the high-risk AI system. That process should aim to identify and mitigate relevant risks of AI systems to health, safety and fundamental rights. The risk management system should be regularly reviewed and updated to ensure its continued effectiveness, as well as the justification and documentation of any significant decisions and actions taken pursuant to this Regulation. This process should ensure that the provider identifies the risks or negative effects and implements mitigation measures for known and reasonably foreseeable risks of AI systems to health, safety and fundamental rights, taking into account their intended purpose and reasonably foreseeable misuse, including potential risks arising from the interaction between the AI system and the environment in which it operates. The risk management system should take the most appropriate risk management measures in light of the current state of the art in AI. When determining the most appropriate risk management measures, the provider should document and explain the choices made and, where appropriate, involve external experts and stakeholders. When determining reasonably foreseeable misuse of high-risk AI systems, the provider should take into account uses of AI systems that, although not directly covered by the intended purpose or set out in the instructions for use, can reasonably be expected to result from easily foreseeable human behaviour in the context of the specific characteristics and use of a particular AI system. Any known or foreseeable circumstances, associated with the use of the high-risk AI system in accordance with its intended purpose or with reasonably foreseeable misuse, that may give rise to risks to health and safety or fundamental rights, should be included in the instructions for use provided by the provider. This is intended to ensure that the deployer is aware of these risks and takes them into account when using the high-risk AI system. The identification and implementation of risk mitigation measures in the event of foreseeable misuse under this Regulation should not require, in order to address them, additional training specific to the high-risk AI system by the provider to address foreseeable misuses. However, providers are encouraged to consider such additional training measures to mitigate reasonably foreseeable misuses, where necessary and appropriate.

(66) Requirements regarding risk management, quality and relevance of data sets used, technical documentation and record keeping, transparency and communication of information to those responsible for deployment, human oversight, robustness, and compliance should apply to high-risk AI systems.
accuracy and cybersecurity. Such requirements are necessary to effectively mitigate risks to health, safety and fundamental rights. In the absence of reasonably available less trade-restrictive measures, such requirements are not unjustified restrictions on trade.

(67) High-quality data and access to high-quality data play an essential role in providing structure and ensuring the functioning of many AI systems, in particular when techniques involving model training are used, with a view to ensuring that the high-risk AI system operates as intended and safely and does not become a source of any form of discrimination prohibited by Union law. Appropriate data management and governance practices need to be in place to ensure that data sets for training, validation and testing are of high quality. Data sets for training, validation and testing, including labels, should be relevant, sufficiently representative and, to the greatest extent possible, error-free and complete in view of the intended purpose of the system. In order to facilitate compliance with Union data protection law, such as Regulation (EU) 2016/679, data management and governance practices should include, in the case of personal data, transparency about the original purpose of the data collection. Data sets should have appropriate statistical properties, including with respect to the persons or groups of persons in relation to whom the high-risk AI system is intended to be used, with particular attention being paid to mitigating potential biases in the data sets that may affect the health and safety of natural persons, have negative impacts on fundamental rights or give rise to any other type of harm.

discrimination prohibited by Union law, especially when output data influences input information for future operations (feedback loops). Biases may, for example, be inherent in the underlying data sets, especially when historical data is used, or generated when systems are deployed in real-world environments. The outputs of AI systems depend on such inherent biases, which tend to increase gradually and thus perpetuate and amplify existing discrimination, in particular with regard to persons belonging to certain vulnerable groups, including racial or ethnic groups. The requirement that data sets, to the greatest extent possible, be complete and error-free should not affect the use of privacy protection techniques in the context of the development and testing of AI systems. In particular, data sets should take into account, to the extent required by their intended purpose, the particular features, characteristics or elements of the specific geographical, contextual, behavioural or functional environment in which the AI system is intended to be used. Requirements related to data governance may be met by using third parties offering certified compliance services, including verification of data governance, data set integrity and data training, validation and testing practices, to the extent that compliance with the data requirements of this Regulation is ensured.

(68) In order to be able to develop and assess high-risk AI systems, certain actors, such as vendors, notified bodies and other relevant entities such as European digital innovation hubs, testing and experimentation facilities and researchers, should have access to and be able to use high-quality datasets in their fields of activity related to this Regulation. Common European data spaces established by the Commission and the facilitation of data sharing between companies and with governments in the public interest will be essential to provide trusted, responsible and non-discriminatory access to high-quality data to train, validate and test AI systems. For example, in the area of health, the European Health Data Space will facilitate non-discriminatory access to health data and the training of AI algorithms on the basis of such datasets in a secure, timely, transparent, trustworthy and privacy-respecting manner, with appropriate institutional governance. Relevant competent authorities, including sectoral ones, that provide or facilitate access to data can also support the provision of high-quality data with which to train, validate and test AI systems.

(69) The right to privacy and protection of personal data must be guaranteed throughout the entire life cycle of the data.
AI system. In this regard, the principles of data minimisation and data protection by design and by default, as set out in Union data protection law, apply when processing personal data. Measures taken by providers to ensure compliance with these principles may include not only anonymisation and encryption, but also the use of technology that allows algorithms to be brought to data and the training of AI systems without the need for transmission between parties or copying of raw or structured data, without prejudice to the data governance requirements set out in this Regulation.

(70) In order to protect the rights of third parties against discrimination that could result from bias in AI systems, providers should – by way of exception, to the extent strictly necessary to ensure the detection and correction of bias associated with high-risk AI systems, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons and after application of all applicable conditions set out in this Regulation, in addition to the conditions set out in Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680 – be able to process also special categories of personal data, as a matter of essential public interest within the meaning of point (g) of Article 9(2) of Regulation (EU) 2016/679 and point (g) of Article 10(2) of Regulation (EU) 2018/1725.

(71) In order to enable traceability of high-risk AI systems, to verify their compliance with the requirements of this Regulation, to monitor their performance and to carry out post-market surveillance, it is essential to have comprehensible information on how they have been developed and on their performance throughout their lifetime. For this purpose, records should be kept and technical documentation should be available containing the information necessary to assess whether the AI system in question complies with the relevant requirements and to facilitate post-market surveillance. Such information should include the general characteristics, capabilities and limitations of the system and the algorithms, data and training, testing and validation processes used, as well as documentation on the relevant risk management system, prepared in a clear and complete manner. The technical documentation should be kept appropriately up-to-date throughout the lifetime of the AI system. In addition, high-risk AI systems should technically allow for the automatic recording of events, by means of log files, throughout the lifetime of the system.

(72) In order to address concerns related to the opacity and complexity of certain AI systems and to assist deployers in meeting their obligations under this Regulation, transparency should be required for high-risk AI systems before they are placed on the market or put into service. High-risk AI systems should be designed in a way that allows deployers to understand how the AI system works, to assess its functionality and to understand its strengths and limitations. High-risk AI systems should be accompanied by appropriate information in the form of instructions for use. Such information should include the characteristics, capabilities and limitations of the operation of the AI system. These would include information on known and foreseeable potential circumstances related to the use of the high-risk AI system, including the actions of the deployer capable of influencing the behaviour and operation of the system, under which the AI system may give rise to risks to health, safety and fundamental rights, on changes that have been predetermined and assessed by the provider for compliance, and on relevant human oversight measures, including measures to facilitate the interpretation of the output results of the AI system by deployers. Transparency, including instructions for use accompanying AI systems, should assist deployers in using the system and making informed decisions. Deployers should, inter alia, be better placed to make the correct choice of the system they intend to use in light of the obligations applicable to them, be informed about the intended and excluded uses, and use the AI system correctly and as appropriate. In order to improve the readability and accessibility of the information included in the instructions for use, illustrative examples should be included where appropriate, for example on limitations and on the intended and excluded uses of the AI system. Providers should ensure that all documentation, including the instructions for use, contains meaningful, comprehensive, accessible and comprehensible information, taking into account the foreseeable needs and knowledge of the intended deployers. The instructions for use should be made available in a language that is easily understood by the intended deployers, as decided by the Member State concerned.

(73) High-risk AI systems should be designed and developed in such a way that natural persons can monitor their operation and ensure that they are used as intended and that their impacts are addressed throughout the lifecycle of the system. To this end, the system provider should define appropriate human oversight measures before the system is placed on the market or put into service. Where appropriate, such measures should ensure, in particular, that the system is subject to operational limitations built into the system itself that cannot be disabled by the system, that the system is responsive to the human operator, and that natural persons entrusted with human oversight have the necessary competence, training and authority to perform that role. It is also essential, where appropriate, to ensure that high-risk AI systems include mechanisms to guide and inform natural persons entrusted with human oversight to make informed decisions about whether, when and how to intervene in order to avoid negative consequences or risks, or to stop the system if it does not operate as intended. Given the enormous consequences for individuals in the event of an incorrect match made by certain biometric identification systems, it is appropriate to establish a requirement for enhanced human oversight for such systems, so that the deployer cannot act or take any decision based on the identification generated by the system unless it has been separately verified and confirmed by at least two natural persons. Such persons could come from one or more entities and include the person operating or using the system. This requirement should not cause unnecessary burden or delay and it could be sufficient if the verifications carried out separately by different persons are automatically recorded in the logs generated by the system. Given the specificities of the areas of law enforcement, migration, border control and asylum, that requirement should not apply where its application is considered disproportionate by Union or national law.

(74) High-risk AI systems should operate consistently throughout their lifecycle and exhibit an appropriate level of accuracy, robustness and cybersecurity, in light of their intended purpose and in accordance with the generally recognised state of the art. The Commission and relevant organisations and stakeholders are encouraged to take due account of mitigating the risks and negative impacts of the AI system. The intended level of operating parameters should be declared in the instructions for use accompanying AI systems. Suppliers are encouraged to communicate such information to those responsible for deployment in a clear and easily understandable manner, without misunderstandings or misleading statements. Union law on legal metrology, including Directives 2014/31/EU (35) and 2014/32/EU (36) of the European Parliament and of the Council, aims to ensure the accuracy of measurements and contribute to the transparency and fairness of commercial transactions. In that context, in cooperation with relevant stakeholders and organisations, such as metrology and benchmarking authorities, the Commission should, as appropriate, encourage the development of benchmarks and measurement methodologies for AI systems. In doing so, the Commission should take note of and engage with international partners working on metrology and relevant AI-related measurement indicators.

(35) Directive 2014/31/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the placing on the market of non-automatic weighing instruments (OJ L 96, 29.3.2014, p. 107).

(36) Directive 2014/32/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the marketing of measuring instruments (OJ L 96, 29.3.2014, p. 149).

(75) Technical robustness is a key requirement for high-risk AI systems, which need to be resilient to harmful or otherwise undesirable behaviour that may arise from limitations in the systems or the environment in which they operate (e.g. errors, failures, inconsistencies or unexpected situations). Technical and organisational measures should therefore be taken to ensure the robustness of high-risk AI systems, for example by designing and developing appropriate technical solutions to prevent or minimise such harmful or undesirable behaviour. Such technical solutions may include, for example, mechanisms that allow the system to safely stop operating (fail-safe plans) in the presence of certain anomalies or when operation occurs outside certain predetermined limits. Failure to take protective measures against such risks could have safety consequences or negatively impact fundamental rights, for example due to wrong decisions or erroneous or biased output results generated by the AI system.

(76) Cybersecurity is critical to ensuring that AI systems are resilient to malicious third parties who, by exploiting vulnerabilities in the system, attempt to alter its use, behavior, or operation or compromise its security properties. Cyberattacks against AI systems can target specific AI assets, such as training data sets (e.g., data poisoning) or trained models (e.g., adversarial attacks or membership inference),

or exploit vulnerabilities in the AI system's digital assets or the underlying ICT infrastructure. Therefore, to ensure a level of cybersecurity appropriate to the risks, providers of high-risk AI systems should take appropriate measures, such as security controls, also taking into account, where appropriate, the underlying ICT infrastructure.

(77) Without prejudice to the requirements related to robustness and accuracy set out in this Regulation, high-risk AI systems falling within the scope of a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, in accordance with that Regulation, may demonstrate compliance with the cybersecurity requirements of this Regulation by complying with the essential cybersecurity requirements set out in that Regulation. Where high-risk AI systems comply with the essential cybersecurity requirements of a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, they should be presumed to comply with the cybersecurity requirements of this Regulation to the extent that satisfaction of those requirements is demonstrated in the EU declaration of conformity issued pursuant to that Regulation, or parts thereof. To that end, the assessment of the cybersecurity risks associated with a product with digital elements classified as a high-risk AI system under this Regulation, carried out pursuant to a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, should take into account the risks to the cyber resilience of an AI system with regard to attempts by unauthorised third parties to alter its use, behaviour or operation, including AI-specific vulnerabilities such as data poisoning or adversarial attacks, as well as, where applicable, risks to fundamental rights, as required by this Regulation.

(78) The conformity assessment procedure set out in this Regulation should be applied in relation to the essential cybersecurity requirements of a product with digital elements regulated by a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and classified as a high-risk AI system under this Regulation. However, this standard should not lead to a reduction in the level of assurance required for critical products with digital elements subject to a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements. Therefore, by way of derogation from this Regulation, high-risk AI systems falling within the scope of this Regulation and which are also considered important critical products with digital elements under a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and to which the conformity assessment procedure based on internal control set out in an Annex to this Regulation applies, are subject to the provisions of a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements for conformity assessment as regards the essential cybersecurity requirements of that Regulation. In such a case, for all other aspects falling within the scope of this Regulation, the provisions of Annex VI to this Regulation on conformity assessment based on internal control should apply. Taking into account the expertise and experience of the European Union Agency for Cybersecurity (ENISA) in cybersecurity policy and the tasks conferred on it by Regulation (EU) 2019/881 of the European Parliament and of the Council [37], the Commission should cooperate with ENISA on issues related to the cybersecurity of AI systems.

[37] 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 information and communications technology cybersecurity certification and repealing Regulation (EU) No.either526/2013 (‘Cybersecurity Regulation’) (OJ L 151, 7.6.2019, p. 15).

(79) It is appropriate that a specific natural or legal person, defined as the provider, assumes the responsibility associated with the placing on the market or putting into service of a high-risk AI system, regardless of whether or not that natural or legal person is the one who designed or developed the system.

(80) As signatories to the Convention on the Rights of Persons with Disabilities, the Union and all Member States are legally obliged to protect persons with disabilities from discrimination and to promote their equality, to ensure that persons with disabilities have access, on an equal basis with others, to information and communications technologies and systems, and to ensure respect for the privacy of persons with disabilities. Given the growing importance and use of AI systems, the application of universal design principles to all new technologies and services should ensure full and equal access for all persons who may be affected by or who may use AI technologies, including persons with disabilities, in a manner that fully takes into account their inherent dignity and diversity. It is therefore essential that providers ensure full compliance with accessibility requirements, including Directive (EU) 2016/2102 of the European Parliament and of the Council [38] and Directive (EU) 2019/882. Providers must ensure compliance with these requirements by design. The necessary measures should therefore be integrated into the design of high-risk AI systems to the extent possible.

(81) The supplier should put in place a robust quality management system, ensure that the necessary conformity assessment procedure is followed, draw up the relevant documentation and establish a robust post-market surveillance system. Suppliers of high-risk AI systems that are subject to obligations relating to quality management systems under the relevant sectoral Union law should have the possibility to integrate the elements of the quality management system set out in this Regulation into the quality management system set out in that sectoral Union law. The complementarity between this Regulation and existing sectoral Union law should also be taken into account in future standardisation activities or in guidance adopted by the Commission in this regard. Public authorities putting high-risk AI systems into service for their own use may adopt and apply rules governing the quality management system within the framework of the quality management system adopted at national or regional level, as appropriate, taking into account the particularities of the sector and the competences and organisation of the public authority concerned.

(82) In order to enable the implementation of this Regulation and to provide a level playing field for operators, it is important to ensure that a person established in the Union can, in any circumstances, provide the authorities with all necessary information on the compliance of an AI system, taking into account the different ways in which digital products can be offered. Therefore, before placing their AI systems on the market in the Union, providers established outside their territory should appoint, by means of a written mandate, an authorised representative located in the Union. The authorised representative plays a key role in ensuring the compliance of high-risk AI systems placed on the market or put into service in the Union by such providers not established in the Union and serves as a contact person established in the Union.

(83) Considering the nature and complexity of the AI value chain and in accordance with the new legislative framework, it is essential to ensure legal certainty and facilitate compliance with this Regulation. It is therefore necessary to clarify the specific role and obligations of relevant operators throughout the AI value chain, such as importers and distributors, who may contribute to the development of AI systems. In certain situations, such operators may perform more than one role at the same time and therefore must cumulatively fulfil all relevant obligations associated with those roles. For example, an operator may act as a distributor and an importer at the same time.

(84) In order to ensure legal certainty, it is necessary to clarify that, under certain specific conditions, any distributor, importer, deployer or other third party should be considered a supplier of a high-risk AI system and should therefore assume all relevant obligations. This would be the case if, for example, that person puts his name or trademark on a high-risk AI system already placed on the market or put into service, without prejudice to contractual agreements stipulating a different allocation of obligations.
This would also be the case if that Party substantially modifies a high-risk AI system that has already been placed on the market or put into service in such a way that the modified system remains a high-risk AI system in accordance with this Regulation, or if it modifies the intended purpose of an AI system, such as a general-purpose AI system, that has already been placed on the market or put into service and is not classified as a high-risk system, in such a way that the modified system becomes a high-risk AI system in accordance with this Regulation. Those provisions should apply without prejudice to more specific provisions set out in certain Union harmonisation legislative acts based on the new legislative framework to be applied in conjunction with this Regulation. For example, the

[38] Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of websites and mobile applications of public sector bodies (OJ L 327, 2.12.2016, p. 1).

Article 16(2) of Regulation (EU) 2017/745, which provides that certain changes should not be considered as modifications to a device that may affect compliance with the applicable requirements, should continue to apply to high-risk AI systems that are medical devices within the meaning of that Regulation.

(85) General-purpose AI systems may be used as high-risk AI systems on their own or as components of high-risk AI systems. Therefore, due to their particular nature and in order to ensure a fair sharing of responsibilities along the entire value chain, providers of such systems, regardless of whether these systems may be used as high-risk AI systems on their own by other providers or as components of high-risk AI systems, and unless otherwise provided for in this Regulation, should cooperate closely with the providers of the relevant high-risk AI systems in order to enable them to comply with the relevant obligations under this Regulation.
as well as with the competent authorities established pursuant to this Regulation.

(86) Where, under the conditions set out in this Regulation, the supplier that initially placed the AI system on the market or put it into service is no longer to be considered as the supplier for the purposes of this Regulation, and where that supplier has not expressly excluded the transformation of the AI system into a high-risk AI system, the first supplier shall nevertheless cooperate closely, provide the necessary information and provide the technical access or other assistance that may reasonably be expected and that is necessary for the fulfilment of the obligations set out in this Regulation, in particular as regards the fulfilment of the conformity assessment of high-risk AI systems.

(87) Furthermore, where a high-risk AI system that is a safety component of a product falling within the scope of a Union harmonisation legislative act based on the new legislative framework is not placed on the market or put into service independently of the product, the manufacturer of the product, as defined in the relevant legislative act, should comply with the obligations imposed on the supplier by this Regulation and, in particular, should ensure that the AI system embedded in the final product complies with the requirements of this Regulation.

(88) Along the AI value chain, numerous parties often supply not only AI systems, tools, and services, but also components or processes that the vendor incorporates into the AI system for various purposes, such as model training, model retraining, model testing and evaluation, integration into the AI system, and so on.softwareor other aspects of model development. Such parties play an important role in the value chain in relation to the provider of the high-risk AI system into which their AI systems, tools, services, components or processes are integrated, and should provide that provider, by written agreement, with the information, capabilities, technical access and other assistance that is necessary, taking into account the generally recognised state of the art, to enable the provider to fully comply with the obligations set out in this Regulation, without compromising its own intellectual property rights or trade secrets.

(89) Third parties making publicly available AI tools, services, processes or components that are not general-purpose AI models should not be required to comply with requirements regarding responsibilities along the AI value chain, in particular as regards the provider that has used or integrated such AI tools, services, processes or components, where access to such AI tools, services, processes or components is subject to a free and open source licence. However, developers of free and open source AI tools, services, processes or components that are not general-purpose AI models should be encouraged to apply widely adopted documentation practices, such as model cards and datasheets, as a way to accelerate the exchange of information along the AI value chain, enabling the promotion of trustworthy AI systems in the Union.

(90) The Commission could develop and recommend voluntary standard contractual clauses between providers of high-risk AI systems and third parties supplying tools, services, components or processes to be used or integrated into high-risk AI systems, in order to facilitate cooperation along the value chain. When developing such voluntary standard contractual clauses, the Commission should also take into account potential contractual requirements applicable in certain sectors or business models.

(91) Given the characteristics of AI systems and the risks associated with their use for security and fundamental rights, including with regard to the need to ensure proper oversight of the operation of an AI system in a real-life environment, it is appropriate to establish specific responsibilities for deployers. In particular, deployers should take appropriate technical and organisational measures to ensure that they use high-risk AI systems in accordance with the instructions for use. In addition, further obligations should be defined in relation to the oversight of the operation of AI systems and record keeping, as appropriate. Deployers should also ensure that persons responsible for implementing the instructions for use and human oversight set out in this Regulation have the necessary competences, in particular an adequate level of literacy,

training and authority in AI to adequately perform such tasks. Such obligations should be without prejudice to other obligations that the deployer has in relation to high-risk AI systems under Union or national law.

(92) This Regulation is without prejudice to the obligation of employers to inform or to inform and consult workers or their representatives, under Union or national law or practice, including Directive 2002/14/EC of the European Parliament and of the Council [39], on the decision to put into service or use AI systems. Workers and their representatives should be informed about the intended deployment of high-risk AI systems in the workplace even if the conditions of the above-mentioned information obligations or information and consultation obligations provided for in other legal instruments are not met. Furthermore, this right to information is ancillary and necessary to the objective of the protection of fundamental rights underlying this Regulation. Therefore, an information requirement to that effect should be laid down in this Regulation, without affecting any existing rights of workers.

(93) While risks related to AI systems may arise from their design, risks may also arise from the use of such systems. Those responsible for deploying a high-risk AI system therefore play a key role in ensuring the protection of fundamental rights, as a complement to the obligations of the provider when developing the AI system. Those responsible for deploying a high-risk AI system are in a best position to understand the specific use to which the high-risk AI system will be put and can therefore identify potential significant risks that were not foreseen at the development stage, by having a more precise knowledge of the context of use and of the persons or groups of persons likely to be affected, including vulnerable groups. Those responsible for deploying high-risk AI systems listed in an Annex to this Regulation also play a key role in informing natural persons and, when making decisions or assisting in making decisions relating to natural persons, should, where appropriate, inform natural persons that they are subject to the use of a high-risk AI system. This information should include the intended purpose and the type of decisions taken. The deployer should also inform natural persons of their right to an explanation under this Regulation. As regards high-risk AI systems used for enforcement purposes, that obligation should be implemented in accordance with Article 13 of Directive (EU) 2016/680.

(94) Any processing of biometric data in connection with the use of an AI system for biometric identification for law enforcement purposes must comply with Article 10 of Directive (EU) 2016/680, which permits such processing only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject and where authorised by Union or Member State law. Such use, where authorised, must also respect the principles set out in Article 4(1) of Directive (EU) 2016/680, such as, inter alia, lawfulness and fair processing, transparency, purpose limitation, accuracy and retention period limitation.

(95) Without prejudice to applicable Union law, in particular Regulation (EU) 2016/679 and Directive (EU) 2016/680, taking into account the intrusive nature of remote biometric identification systems, the use of such systems should be subject to safeguards. Remote biometric identification systems should always be used in a proportionate and legitimate manner, to the extent strictly necessary and therefore selectively as regards the persons to be identified, the location and temporal scope and on the basis of a limited set of data from lawfully obtained video recordings. In any event, remote biometric identification systems should not be used in the context of law enforcement in such a way as to result in indiscriminate surveillance. The conditions for remote biometric identification should in no case serve to circumvent the conditions of the prohibition and the strict exceptions applicable to real-time remote biometric identification.

(96) In order to effectively ensure the protection of fundamental rights, those responsible for the deployment of high-risk AI systems that are bodies governed by public law, or private entities providing public services and those responsible for the deployment of certain high-risk AI systems listed in an Annex to this Regulation, such as banking or insurance entities, should carry out a fundamental rights impact assessment before their deployment. Some services important to individuals that are of a public nature may also be provided by private entities. Private entities providing these public services are linked to functions of public interest, for example in the field of education, healthcare, social services, housing and the administration of justice. The objective of the fundamental rights impact assessment is for the deployer to identify the specific risks to the rights of individuals or groups of individuals likely to be affected and to define the measures to be taken if those risks materialise. The impact assessment should

[39] Directive 2002/14/EC of the European Parliament and of the Council of 11 March 2002 establishing a general framework for the on information and consultation of workers in the European Community (OJ L 80, 23.3.2002, p. 29).

be carried out prior to the deployment of the high-risk AI system and should be updated when the deployer considers that any of the relevant factors have changed. The impact assessment should identify the relevant processes of the deployer in which the high-risk AI system will be used in line with its intended purpose and should include a description of the time frame and frequency in which the system is intended to be used, as well as the specific categories of natural persons and groups of persons likely to be affected by the use of the high-risk AI system in that specific context of use. The assessment should also identify the specific risks of harm likely to affect the fundamental rights of those persons or groups. When carrying out this assessment, the deployer should take into account information relevant to an appropriate impact assessment, including, for example, information provided by the provider of the high-risk AI system in the instructions for use. In light of the identified risks, deployers should identify the measures to be taken in the event that such risks materialise, including, for example, governance systems for that specific context of use, such as human oversight mechanisms in accordance with the instructions for use, grievance and redress procedures, as these could be key to mitigating risks to fundamental rights in specific use cases. After carrying out such an impact assessment, the deployer should notify the relevant market surveillance authority. Where appropriate, in order to gather the relevant information needed to carry out the impact assessment, deployers of a high-risk AI system, in particular where the AI system is used in the public sector, may involve relevant stakeholders, such as representatives of groups of people likely to be affected by the AI system, independent experts or civil society organisations, in carrying out such impact assessments and in designing the measures to be taken in the event of risks materialising. The European Artificial Intelligence Office (hereinafter referred to as the 'AI Office') should develop a model questionnaire in order to facilitate compliance and reduce the administrative burden for those responsible for deployment.

(97) The concept of general-purpose AI models should be clearly defined and distinguished from the concept of AI systems in order to ensure legal certainty. The definition should be based on the essential functional characteristics of a general-purpose AI model, in particular generality and the ability to competently perform a wide variety of differentiated tasks. These models are typically trained using large volumes of data and through various methods, such as self-supervised, unsupervised or reinforcement learning. General-purpose AI models can be introduced to the market in various ways, for example, through libraries, application programming interfaces (APIs), as a direct download or as a physical copy. These models can be modified or refined and transformed into new models. Although AI models are essential components of AI systems, they do not constitute AI systems in themselves. AI models require the addition of other components, such as a user interface, to become AI systems. AI models are typically integrated into AI systems and form part of such systems. This Regulation lays down specific rules for general-purpose AI models and for general-purpose AI models that pose systemic risks, which should also apply when these models are integrated into an AI system or are part of an AI system. It should be understood that the obligations of providers of general-purpose AI models should apply once the general-purpose AI models are placed on the market. Where the provider of a general-purpose AI model integrates a proprietary model into a proprietary AI system that is placed on the market or put into service, that model should be deemed to have been placed on the market and therefore the obligations set out in this Regulation in relation to models should continue to apply, in addition to those set out in relation to AI systems. In any case, the obligations set out in relation to models should not apply where a proprietary model is used in purely internal processes that are not essential for providing a product or service to a third party and the rights of natural persons are not affected. Taking into account its potential to cause significant adverse effects, General-purpose AI models with systemic risk should always be subject to the relevant obligations set out in this Regulation. The definition should not include AI models used prior to their placing on the market solely for research, development and prototyping activities. This is without prejudice to the obligation to comply with this Regulation when, after such activities, the model is placed on the market.

(98) Although the generality of a model could also be determined by, among other things, a set of parameters, models that have at least a billion parameters and have been trained on a large volume of data using self-supervision at scale should be considered to have a significant degree of generality and competently perform a wide variety of discrete tasks.

(99) Large generative AI models are a typical example of a general-purpose AI model, as they allow for the flexible generation of content, for example in text, audio, image or video format, which can be easily adapted to a wide range of differentiated tasks.

(100) Where a general-purpose AI model is integrated into or forms part of an AI system, this system should be considered a general-purpose AI system when, due to this integration, the system has the ability to serve multiple purposes. A general-purpose AI system can be used directly and integrated into other AI systems.

(101) Providers of general-purpose AI models have a particular role and responsibility along the AI value chain, as the models they provide may form the basis of various downstream systems, which are often provided by downstream providers who need to have a good understanding of the models and their capabilities, both to enable the integration of those models into their products and to fulfil their obligations under this Regulation or other regulations. Therefore, proportionate transparency measures should be put in place, including by developing and keeping up-to-date documentation and providing information on the general-purpose AI model for use by downstream providers. The provider of the general-purpose AI model should develop and keep up-to-date technical documentation in order to make it available, upon request, to the AI Office and to the competent national authorities. The minimum elements to be contained in that documentation should be set out in specific annexes to this Regulation. The Commission should be empowered to amend those annexes by means of delegated acts in the light of technological developments.

(102) Thesoftwareand data, including models, disclosed under a free and open source license that allows open sharing and user access, or modified versions of such data. softwareand such data, or freely use, modify and redistribute it, can contribute to research and innovation on the market and can offer important growth opportunities for the Union economy. General-purpose AI models disclosed under a free and open-source licence should be considered to ensure high levels of transparency and openness if their parameters, including weights, information on the model architecture and information on the use of the model, are made publicly available. The licence should be considered free and open-source when it allows users to run, copy, distribute, study, modify and improve the model.softwareand data, including models provided that the original supplier of the model is cited, if identical or comparable distribution conditions are respected.

(103) Free and open source AI components include thesoftwareand data, including general-purpose AI models and models, tools, services and processes of an AI system. Free and open-source AI components may be supplied through different channels, including the possibility of developing them in open repositories. For the purposes of this Regulation, AI components that are supplied for consideration or are otherwise monetized, such as through the provision of technical support or other services in relation to the AI component, whether through a platform or a service, shall be considered as such components.softwareor by other means, or by using personal data for purposes other than solely related to improving the security, compatibility or interoperability of thesoftware,except in the case of transactions between micro-enterprises, they should not be eligible for the exceptions provided for free and open source AI components. The availability of an AI component through open repositories should not, in itself, constitute monetisation.

(104) Providers of general-purpose AI models disclosed under a free and open-source licence whose parameters, including weights, information on the architecture of the model and information on the use of the model, are made publicly available should be subject to exceptions from the transparency requirements imposed on general-purpose AI models, unless they can be considered to present a systemic risk, in which case the fact that the model is transparent and is accompanied by an open-source licence should not be considered a sufficient reason for it to be exempted from the obligations set out in this Regulation. In any event, since the disclosure of general-purpose AI models under a free and open-source licence does not necessarily reveal substantial information about the dataset used to train or fine-tune the model or how compliance with copyright law was ensured, the exception provided for general-purpose AI models in relation to compliance with transparency requirements should not exempt from the obligation to provide a summary of the content used for training the model or from the obligation to adopt guidelines for compliance with Union copyright law, in particular for identifying and respecting the reservation of rights provided for in Article 4(3) of Directive (EU) 2019/790 of the European Parliament and of the Council [40].

(105) General-purpose AI models, in particular large generative AI models, capable of generating text, images and other content present unique opportunities for innovation, but also challenge artists, authors and other creators and the way their creative content is created, distributed, used and consumed. Developing and training these models requires access to large amounts of text, images, videos and other data. Text and data mining techniques can be widely used in this context for the retrieval and analysis of such content, which may be protected by copyright and related rights. Any use of copyrighted content requires the authorisation of the rights holder concerned, unless relevant copyright exceptions and limitations apply. Directive (EU) 2019/790 introduced exceptions and limitations that allow reproductions and extractions of works and other subject matter for text and data mining purposes in certain circumstances. Under

[40] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the digital single market and amending Directives 96/9/EC and 2001/29/EC (OJ L 130, 17.5.2019, p. 92).

Under these rules, copyright holders may choose to reserve their rights in relation to their works or other subject matter to prevent text and data mining, unless the purpose of the work is scientific research. Where the copyright holder has appropriately reserved the right to opt out, providers of general-purpose AI models must obtain the copyright holder's permission to conduct text and data mining on such works.

(106) Providers placing general-purpose AI models on the Union market should ensure compliance with the relevant obligations set out in this Regulation. To that end, providers of general-purpose AI models should adopt guidelines for compliance with Union copyright and related rights law, in particular for detecting and complying with the reservation of rights expressed by rightholders pursuant to Article 4(3) of Directive (EU) 2019/790. Any provider placing a general-purpose AI model on the Union market should comply with this obligation, regardless of the jurisdiction in which the relevant copyright acts underpinning the training of such general-purpose AI models take place. This measure is necessary to ensure a level playing field between providers of general-purpose AI models that prevents a provider from gaining a competitive advantage on the Union market by applying less stringent copyright rules than those provided for in the Union.

(107) In order to increase transparency regarding the data used in the pre-training and training of general-purpose AI models, including texts and data protected by copyright law, it is appropriate for providers of such models to prepare and make publicly available a sufficiently detailed summary of the content used for the training of the general-purpose AI model. This summary should take due account of the need to protect trade secrets and confidential business information, while being generally comprehensive in scope rather than technically detailed, in order to facilitate parties with legitimate interests, including copyright holders, to exercise and enforce their rights under Union law, for example by listing the main data sets or collections that have been used to train the model, such as private or public big data archives or databases, and by providing a descriptive explanation of other data sources used. It is appropriate for the IA Office to provide a template for the summary, which should be simple and effective and allow the provider to provide the required summary in a descriptive form.

(108) As regards the obligations imposed on providers of general-purpose AI models to adopt guidelines for compliance with Union copyright law and to make publicly available a summary of the content used for training, the AI Office should monitor whether the provider has complied with those obligations without verifying or carrying out a work-by-work assessment of the training data for copyright compliance. This Regulation does not affect compliance with the copyright rules provided for in Union law.

(109) Compliance with the obligations applicable to providers of general-purpose AI models should be proportionate and appropriate to the type of model provider. Persons who develop or use models for non-professional or scientific research purposes should be exempted from the compliance obligation. However, such persons should be encouraged to comply voluntarily with these requirements. Without prejudice to Union copyright law, compliance with those obligations should take due account of the size of the provider and allow for simplified forms of compliance for SMEs, including start-ups, which should not entail excessive costs or discourage the use of such models. In the event of modifications or adjustments to a model, the obligations of providers of general-purpose AI models should be limited to that modification or adjustments, for example by supplementing existing technical documentation with information on the modifications, including new sources of training data, in order to comply with the value chain obligations set out in this Regulation.

(110) General-purpose AI models may pose systemic risks, for example, any actual or reasonably foreseeable negative effects in relation to serious accidents, disruptions of critical sectors and serious consequences for public health and safety, any actual or reasonably foreseeable negative effects on democratic processes and public and economic security or the dissemination of unlawful, false or discriminatory content. It should be understood that systemic risks increase with the capabilities and reach of the models, may arise throughout the lifecycle of the model and are influenced by the conditions of misuse, the reliability of the model, the fairness and security of the model, the level of autonomy of the model, its access to tools, novel or combined modalities, dissemination and distribution strategies, the possibility of overriding safeguards and other factors. In particular, international approaches to date have established the need to pay attention to risks arising from potential intentional misuse or control problems related to harmonization with unintended human intent, to chemical, biological, radiological and nuclear risks, as well as ways in which barriers to entry can be reduced, as well as

for the development, design, acquisition or use of weapons; offensive cyber capabilities, such as the ways in which vulnerabilities can be discovered, exploited or operationally used; the effects of interaction and tool use, including, for example, the ability to control physical systems and interfere with the operation of critical infrastructure; the risks arising from models making copies of themselves or "self-replicating" or training other models; the ways in which models can give rise to harmful biases and discrimination that pose risks to individuals, communities or societies; the facilitation of disinformation or infringement of privacy, which threaten democratic values and human rights; the risk that a single event could set off a chain reaction with significant negative effects that could even affect an entire city, an entire field of activity or an entire community.

(111) It is appropriate to establish a methodology for the classification of general-purpose AI models as general-purpose AI models with systemic risks. Since systemic risks arise from particularly high capabilities, a general-purpose AI model should be considered to present systemic risks if it has high-impact capabilities – assessed using appropriate technical tools and methodologies – or significant impacts on the internal market due to its reach. High-impact capabilities in general-purpose AI models are capabilities that match or exceed the capabilities shown by the most advanced general-purpose AI models. The introduction of a model on the market or the interactions of deployers with it allow a better understanding of the set of its capabilities. According to the state of the art at the time of the entry into force of this Regulation, the cumulative amount of computation used for the training of the general-purpose AI model, measured in floating-point operations, is one of the relevant proxies for the capabilities of the model. The cumulative amount of computation used for training includes computations used in the various activities and methods intended to improve the model's capabilities prior to deployment, such as pre-training, synthetic data generation, and fine-tuning. Therefore, an initial threshold of floating-point operations should be established that, if reached by a general-purpose AI model, would lead to a presumption that the model is a general-purpose AI model with systemic risks. This threshold should be adjusted to reflect technological and industry changes, such as algorithmic improvements or increased hardware efficiency, and should be supplemented by benchmarks and indicators of model capability. To inform this, the AI Office should engage with the scientific community, industry, civil society, and other experts. The thresholds, as well as the tools and benchmarks for assessing high-impact capabilities, should be able to reliably predict the generality, capabilities and associated systemic risk of general-purpose AI models, and could take into account the way in which the model will be introduced to the market or the number of users it could affect. To complement this system, the Commission should be able to adopt individual decisions designating a general-purpose AI model as a general-purpose AI model with systemic risk if it is determined that the model has capabilities or impacts equivalent to those reflected by the set threshold.That decision should be taken on the basis of an overall assessment of the criteria for the designation of general-purpose AI models with systemic risk set out in an Annex to this Regulation, such as the quality or size of the training dataset, the number of professional and end-users, its input and output modes, its level of autonomy and scalability or the tools to which it has access. Upon a reasoned request from a provider whose model has been designated as a general-purpose AI model with systemic risk, the Commission should take into account the request and may decide to reassess whether the general-purpose AI model can continue to be considered as posing systemic risks.

(112) It is also necessary to clarify a procedure for the classification of a general-purpose AI model with systemic risks. A general-purpose AI model that meets the applicable threshold for high-impact capabilities should be presumed to be a general-purpose AI model with systemic risk. The provider should send a notification to the AI Office no later than two weeks after the requirements are met or it becomes known that a general-purpose AI model will meet the requirements leading to the presumption. This is particularly relevant in relation to the floating-point operations threshold, as training general-purpose AI models requires considerable planning including pre-allocation of computational resources and therefore providers of general-purpose AI models may know whether their model will meet the threshold before the end of training. In the context of such notification, the provider must be able to demonstrate that, due to its specific characteristics, a general-purpose AI model does not exceptionally present systemic risks and should therefore not be classified as a general-purpose AI model with systemic risks. Such information is valuable for the AI Office to anticipate the introduction of general-purpose AI models with systemic risks on the market and for providers to be able to start collaborating with the AI Office at an early stage. Such information is particularly important when a general-purpose AI model is planned to be disclosed as a general-purpose AI model.

open source model, since following the disclosure of open source models, it may be more difficult to implement the measures necessary to ensure compliance with the obligations set out in this Regulation.

(113) If the Commission finds that a general-purpose AI model of which it was not aware or which was not notified to it by the relevant provider qualifies for classification as a general-purpose AI model with systemic risk, the Commission should be empowered to designate it. In addition to the oversight activities of the AI Office, a qualified alert system should ensure that the AI Office is informed by the scientific expert group of the existence of general-purpose AI models that could be classified as general-purpose AI models with systemic risk.

(114) Providers of general-purpose AI models presenting systemic risks should be subject, in addition to the obligations imposed on providers of general-purpose AI models, to obligations aimed at detecting and mitigating such risks and ensuring an adequate level of cybersecurity protection, regardless of whether those models are offered as stand-alone models or are integrated into AI systems or products. In order to achieve those objectives, this Regulation should require providers to carry out the necessary assessments of the models, in particular before the first placing on the market, and for example to carry out and document adversary simulation tests, including, where appropriate, by means of independent external testing or internal testing. Furthermore, providers of general-purpose AI models with systemic risks should continuously assess and mitigate systemic risks, for example by establishing risk management policies, such as accountability and governance processes, implementing post-market surveillance, taking appropriate measures throughout the model lifecycle, and cooperating with relevant actors along the AI value chain.

(115) Providers of general-purpose AI models with systemic risks should assess and mitigate potential systemic risks. If, despite efforts to detect and prevent risks related to a general-purpose AI model that may present systemic risks, the development or use of the model leads to a serious incident, the provider of the general-purpose AI model should, without undue delay, follow up on the incident and communicate all relevant information and possible remedial measures to the Commission and the competent national authorities. Furthermore, providers should ensure that the model and its physical infrastructure, if applicable, have an adequate level of cybersecurity protection throughout the lifecycle of the model. Cybersecurity protection related to systemic risks associated with malicious use or attacks should take due account of accidental model leaks, unauthorised disclosures, circumvention of security measures and defence against cyberattacks, unauthorised access or model theft. Such protection could be facilitated by securing the model weights, algorithms, servers and data sets, for example, through operational security measures for information security, specific cybersecurity measures, appropriate and established technical solutions and cyber and physical access controls, depending on the relevant circumstances and existing risks.

(116) The AI Office should encourage and facilitate the development, review and adaptation of codes of good practice, taking into account international approaches. All providers of general-purpose AI models could be invited to participate. To ensure that codes of practice reflect the current state of the art and take due account of different perspectives, the AI Office should engage with relevant national competent authorities and, where appropriate, may consult civil society organisations and other relevant stakeholders and experts, including the Scientific Expert Group, regarding the development of such codes. Codes of practice should cover obligations for providers of general-purpose AI models and for general-purpose AI models presenting systemic risks. Furthermore, with regard to systemic risks, codes of practice should help establish a risk taxonomy listing the type and nature of systemic risks at Union level, including their sources. Codes of practice should also focus on specific risk assessment and mitigation measures.

(117) Codes of practice should be a key tool for the proper implementation of the obligations under this Regulation for providers of general-purpose AI models. Providers should be able to rely on codes of practice to demonstrate compliance with the obligations. By means of implementing acts, the Commission may decide to adopt a code of practice and give it general validity within the Union or, alternatively, to establish common rules for the implementation of the relevant obligations if, by the time this Regulation becomes applicable, a code of practice has not been finalised or is not considered appropriate by the AI Office. Once a code of practice has been finalised, the Commission may decide to adopt a code of practice and give it general validity within the Union or, alternatively, to establish common rules for the implementation of the relevant obligations if, by the time this Regulation becomes applicable, a code of practice has not been finalised or is not considered appropriate by the AI Office.

Where a harmonised standard has been published and is deemed suitable by the AI Office to cover the relevant obligations, compliance with a European harmonised standard should give providers the presumption of conformity. Furthermore, providers of general-purpose AI models should be able to demonstrate compliance using appropriate alternative means if codes of good practice or harmonised standards are not available, or if they choose not to rely on them.

(118) This Regulation regulates AI systems and AI models by imposing certain requirements and obligations on relevant market players placing them on the market, putting them into service or using them in the Union, thereby complementing the obligations of intermediary service providers integrating such systems or models into their services regulated by Regulation (EU) 2022/2065. To the extent that such systems or models are integrated into very large online platforms or very large online search engines that have been designated, they are subject to the risk management framework set out in Regulation (EU) 2022/2065. Therefore, the relevant obligations under this Regulation should be presumed to have been fulfilled unless significant systemic risks not covered by Regulation (EU) 2022/2065 arise and are identified in such models. In this context, providers of very large online platforms and very large online search engines are obliged

to assess potential systemic risks arising from the design, operation and use of their services, including how the design of the algorithmic systems used in the service may contribute to such risks, as well as systemic risks arising from potential misuse. Such providers are also obliged to adopt appropriate risk mitigation measures while respecting fundamental rights.

(119) Taking into account the rapid pace of innovation and technological evolution of digital services falling within the scope of different instruments of Union law, in particular taking into account the use and perception of their recipients, AI systems subject to this Regulation may be provided as intermediary services, or parts thereof, within the meaning of Regulation (EU) 2022/2065, which should be interpreted in a technologically neutral manner. For example, AI systems may be used to provide online search engines, in particular to the extent that an AI system, such as an online chatbot, searches, in principle, all websites, then incorporates the results into its existing knowledge and uses the updated knowledge to generate a single output combining different sources of information.

(120) Furthermore, the obligations imposed on providers and those responsible for the deployment of certain AI systems in this Regulation to enable the detection and disclosure of artificially generated or manipulated outputs of such systems are particularly relevant to facilitate the effective application of Regulation (EU) 2022/2065. This applies in particular to the obligations of providers of very large online platforms or very large online search engines to detect and mitigate systemic risks that may arise from the disclosure of artificially generated or manipulated content, in particular the risk of actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, including through disinformation.

(121) Standardisation should play a key role in providing technical solutions to suppliers to ensure compliance with this Regulation, in line with the current state of the art, in order to promote innovation as well as competitiveness and growth in the single market. Compliance with the harmonised standards defined in point (c) of Article 2 of Regulation (EU) No 1289/2008 is essential.either1025/2012 of the European Parliament and of the Council [41], which are generally expected to reflect the current state of the art, should be a means for providers to demonstrate compliance with the requirements of this Regulation. Therefore, a balanced representation of the interests of all relevant stakeholders, in particular SMEs, consumer organisations and social and environmental stakeholders, should be encouraged in the development of standards, in accordance with Articles 5 and 6 of Regulation (EU) No 1799/2008.either1025/2012. In order to facilitate compliance, the Commission should issue requests for standardisation without undue delay. When preparing the request for standardisation, the Commission should consult the Advisory Forum and the IA Council to obtain relevant expertise. However, in the absence of relevant references to harmonised standards, the Commission should be able, by means of implementing acts and after consulting the Advisory Forum, to establish common specifications for certain requirements provided for in this Regulation. Common specifications should be an exceptional alternative solution to facilitate the obligation of the provider to comply with the requirements of this Regulation where none of the European standardisation organisations has accepted the request for standardisation, where the relevant harmonised standards insufficiently address fundamental rights concerns, where harmonised standards do not comply with the request or where there are delays in the adoption of an appropriate harmonised standard. Where such delays in the adoption of a harmonised standard are due to the technical complexity of that standard, the Commission should be able to adopt a common specification.

[41] Regulation (EU) No.either1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1025/2012 of the European Parliament and of the Council.either1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

The Commission should take this into account before considering establishing common specifications. The Commission is encouraged to cooperate with international partners and international standardisation bodies when developing common specifications.

(122) It is appropriate that, without prejudice to the use of harmonised standards and common specifications, providers of a high-risk AI system that has been trained and tested on data reflecting the specific geographical, behavioural, contextual or functional environment in which the AI system is intended to be used should be presumed to comply with the relevant measure provided for in the data governance requirement set out in this Regulation. Without prejudice to the requirements related to robustness and accuracy set out in this Regulation, in accordance with Article 54(3) of Regulation (EU) 2019/881, high-risk AI systems that have a certification or a declaration of conformity under a cybersecurity certification scheme pursuant to that Regulation and the references of which have been published in the Regulation should be presumed to comply with the relevant measure provided for in the data governance requirement set out in this Regulation.Official Journal of the European Unioncomply with the cybersecurity requirement of this Regulation to the extent that the cybersecurity certificate or declaration of conformity, or parts thereof, address that requirement. This is without prejudice to the voluntary nature of such cybersecurity scheme.

(123) In order to ensure that high-risk AI systems are highly reliable, such systems should be subject to a conformity assessment before being placed on the market or put into service.

(124) In order to minimise the burden on operators and to avoid possible duplication, it is appropriate, for high-risk AI systems associated with products regulated by existing Union harmonisation legislation based on the new legislative framework, that the conformity of such AI systems with the requirements set out in this Regulation be assessed within the framework of the conformity assessment already provided for in that legislation. Therefore, the applicability of the requirements of this Regulation should not affect the specific logic, methodology or general structure of the conformity assessment provided for in the relevant Union harmonisation legislative acts.

(125) Given the complexity of high-risk AI systems and the risks associated with them, it is important to develop an appropriate conformity assessment procedure for high-risk AI systems involving notified bodies, referred to as ‘third-party conformity assessment’. However, given the current experience of professionals carrying out pre-market certification in the field of product safety and the different nature of the risks involved, it is appropriate to limit, at least in the initial phase of application of this Regulation, the scope of external conformity assessments to high-risk AI systems that are not associated with products. Consequently, the conformity assessment of such systems should, as a rule, be carried out by the supplier under its own responsibility, with the sole exception of AI systems that are intended to be used for biometrics.

(126) In order to be able to carry out third-party conformity assessments when required, national competent authorities should notify notified bodies pursuant to this Regulation, provided that they meet a number of requirements, in particular as regards their independence, competence and absence of conflicts of interest, as well as appropriate cybersecurity requirements. National competent authorities should send the notification of those bodies to the Commission and to the other Member States through the electronic notification system developed and managed by the Commission in accordance with Article R23 of Annex I to Decision No 1999/2002.either768/2008/EC.

(127) In line with the Union's commitments under the World Trade Organisation Agreement on Technical Barriers to Trade, it is appropriate to facilitate the mutual recognition of the results of conformity assessments carried out by competent conformity assessment bodies, irrespective of the territory in which they are established, provided that such conformity assessment bodies established under the law of a third country comply with the applicable requirements of this Regulation and the Union has concluded an agreement to that effect. In this context, the Commission should actively explore possible international instruments to that effect and, in particular, seek to conclude mutual recognition agreements with third countries.

(128) In line with the commonly established concept of ‘substantial modification’ of products covered by Union harmonisation legislation, it is appropriate that whenever a change occurs that may affect the compliance of a high-risk AI system with this Regulation (for example, a change in operating system or architecture),software)or where the intended purpose of the system changes, that AI system is considered a new AI system that must be subject to a new conformity assessment. However, changes to the algorithm and operation of AI systems that continue to “learn” after they are placed on the market or put into service, namely by automatically adapting the way they perform their functions, should not constitute a substantial modification, provided that such changes have been predetermined by the supplier and have been assessed at the time of the conformity assessment.

(129) High-risk AI systems should bear the CE marking to attest their compliance with this Regulation and thus be able to move freely within the internal market. For high-risk AI systems embedded in a product, a physical CE marking should be affixed, which may be supplemented by a digital CE marking. For high-risk AI systems that are only provided digitally, a digital CE marking should be used. Member States should not create unjustified obstacles to the placing on the market or putting into service of high-risk AI systems that comply with the requirements set out in this Regulation and bear the CE marking.

(130) Under certain conditions, the rapid availability of innovative technologies may be crucial for the health and safety of persons, the protection of the environment and climate change mitigation, and for society as a whole. It is therefore appropriate that market surveillance authorities may authorise, on exceptional grounds of public security or with a view to protecting the life and health of natural persons, the environment and critical assets of industry and infrastructure, the placing on the market or putting into service of AI systems that have not been subject to a conformity assessment. In duly justified situations provided for in this Regulation, enforcement authorities or civil protection authorities may put into service a specific high-risk AI system without authorisation from the market surveillance authority, provided that authorisation is requested during or after use without undue delay.

(131) In order to facilitate the work of the Commission and the Member States in the field of AI and to increase transparency for the public, providers of high-risk AI systems that are not associated with products falling within the scope of relevant and applicable Union harmonisation legislation and providers that consider that any of the AI systems listed in the high-risk use cases in an Annex to this Regulation are not high-risk on the basis of a derogation should be required to register and to register information about their AI systems in an EU database, established and managed by the Commission. Before using such an AI system listed in the high-risk use cases in an Annex to this Regulation, those responsible for deploying high-risk AI systems that are public authorities, bodies, offices or agencies should register in that database and select the system they intend to use. Such registration should be possible for other deployers on a voluntary basis. This section of the EU database should be publicly accessible and free of charge, the information should be easy to navigate, and should be comprehensible and machine-readable. The EU database should also be user-friendly, for example by providing search functionalities, including through keywords, allowing the general public to find the information to be submitted for the registration of high-risk AI systems and relating to the use cases of high-risk AI systems referred to in an Annex to this Regulation, to which high-risk AI systems correspond. Any substantial modifications to high-risk AI systems should also be registered in the EU database. For high-risk AI systems in the field of law enforcement and migration management, asylum and border control, registration obligations should be fulfilled in a secure non-public section of the EU database. Access to that section should be strictly limited to the Commission and market surveillance authorities as regards their national section of that database. High-risk AI systems in the field of critical infrastructure should only be registered at national level. The Commission should be the controller of the EU database, in accordance with Regulation (EU) 2018/1725. In order to ensure the full functionality of the EU database once it is operational, the procedure for its establishment should comprise the development of functional specifications by the Commission and the drafting of an independent audit report.When exercising its duties as controller of the EU database, the Commission must take into account cybersecurity risks. In order to maximise the availability and use of the EU database by the public, the EU database and the information provided through it must comply with the requirements set out in Directive (EU) 2019/882.

(132) Certain AI systems intended to interact with natural persons or generate content may pose specific risks of impersonation or deception, regardless of whether they meet the conditions to be considered as high risk or not. Therefore, the use of such systems should be subject, in certain circumstances, to specific transparency obligations, without prejudice to the applicable requirements and obligations.
to high-risk AI systems and to specific exceptions to take into account the special needs of ensuring compliance with the Law. In particular, natural persons should be notified that they are interacting with an AI system, except where it would be obvious from the point of view of a normally informed and reasonably observant and circumspect natural person, taking into account the circumstances and context of use. When applying this obligation, account should be taken of the characteristics of natural persons belonging to vulnerable groups due to their age or disability to the extent that the AI system is intended to interact also with such groups. In addition, natural persons should be notified when they are exposed to AI systems that, through the processing of their biometric data, may determine or infer their emotions or intentions or place them in specific categories. These specific categories may relate to aspects such as sex, age, hair colour, eye colour, tattoos, personal features, ethnic origin or personal preferences and interests. This information and these notifications should be provided in formats accessible to persons with disabilities.

(133) A variety of AI systems can generate large amounts of synthetic content that is increasingly difficult for humans to distinguish from authentic human-generated content. The wide availability and increasing capabilities of such systems have significant implications for the integrity of and trust in the information ecosystem, giving rise to new risks of disinformation and manipulation at scale, fraud, identity theft and deception of consumers. In view of these effects, rapid technological development and the need for new methods and techniques to ensure traceability of the origin of information, it is appropriate to require providers of such systems to integrate technical solutions that allow marking, in a machine-readable format, and detecting that the output result has been generated or manipulated by an AI system and not by a human. Such techniques and methods should be sufficiently reliable, interoperable, effective and robust, to the extent technically feasible, taking into account available techniques or a combination of such techniques, such as watermarking, metadata identification, cryptographic methods to prove the provenance and authenticity of content, registration methods, fingerprinting or other techniques, as appropriate. When implementing this obligation, providers should also take into account the specificities and limitations of different types of content and relevant technological and market developments in that area, as reflected in generally recognised state of the art. Such techniques and methods may be implemented at the AI system level or at the AI model level, including general-purpose AI models generating content, thereby facilitating compliance with this obligation by the downstream provider of the AI system. In order to ensure proportionality, it is appropriate to provide that this marking obligation does not apply to AI systems that perform a standard editing support function or do not substantially alter the input data provided by the deployer or its semantics.

(134) In addition to the technical solutions used by AI system providers, deployers who use an AI system to generate or manipulate AI-generated or manipulated image, audio or video content that substantially resembles real persons, objects, places, entities or events and that may mislead a person into believing that they are authentic or true-to-life (ultraspoofing) should also make public, in a clear and distinguishable manner, that this content has been artificially created or manipulated by labelling the output results generated by the AI accordingly and indicating their artificial origin. Compliance with this transparency obligation should not be interpreted as indicating that the use of the AI system or its output results hinder the right to freedom of expression and the right to freedom of the arts and sciences, as guaranteed by the Charter, in particular where the content forms part of a manifestly creative, satirical, artistic, fictional or similar work or programme, subject to appropriate safeguards for the rights and freedoms of third parties. In such cases, the transparency obligation in relation to impersonations set out in this Regulation is limited to disclosing the existence of such content generated or manipulated in an appropriate manner that does not hinder the normal presentation and enjoyment of the work, including its exploitation and use, while preserving the usefulness and quality of the work. Furthermore, a similar disclosure obligation should also be provided for in relation to text generated or manipulated by AI to the extent that it is published for the purpose of informing the public on matters of public interest, unless the AI-generated content has been subject to a human review or editorial control process and a natural or legal person exercises editorial responsibility for the publication of the content.

(135) Without prejudice to the mandatory nature and full applicability of transparency obligations, the Commission may also encourage and facilitate the development of Union-wide codes of good practice in order to facilitate the effective implementation of obligations regarding the detection and labelling of artificially generated or manipulated content, including to support practical arrangements for making detection mechanisms accessible, where appropriate, and to facilitate cooperation with other actors in the value chain, by disseminating content or verifying its authenticity and provenance, in order to enable the public to effectively distinguish AI-generated content.

(136) The obligations imposed on providers and those responsible for the deployment of certain AI systems in this Regulation to enable the detection and disclosure of artificially generated or manipulated outputs of such systems are particularly relevant to facilitate the effective application of Regulation (EU) 2022/2065. This applies in particular to the obligations of providers of very large online platforms or very large online search engines to detect and mitigate systemic risks that may arise from the disclosure of artificially generated or manipulated content, in particular the risk of actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, such as through disinformation. The requirement to label content generated by AI systems under this Regulation is without prejudice to the obligation under Article 16(6) of Regulation (EU) 2022/2065 for hosting service providers to process notifications they receive about unlawful content under Article 16(1) of that Regulation and should not influence the assessment and decision on the unlawfulness of the content in question. Such assessment should be made solely with reference to the rules governing the legality of the content.

(137) Compliance with the transparency obligations applicable to AI systems falling within the scope of this Regulation should not be interpreted as an indicator that the use of the AI system or its output results is lawful under this Regulation or other provisions of Union and Member State law, and should be without prejudice to other transparency obligations applicable to controllers of the deployment of AI systems laid down in Union or national law.

(138) AI is a rapidly evolving family of technologies that requires regulatory oversight and a safe and controlled space for experimentation, as well as ensuring responsible innovation and the integration of appropriate ethical safeguards and risk mitigation measures. In order to achieve a legal framework that promotes innovation, is time-tested and resilient to disruption, Member States should ensure that their competent national authorities establish at least one national AI sandbox to facilitate the development and testing of innovative AI systems under strict regulatory oversight before they are placed on the market or put into service. Member States could also fulfil this obligation by participating in existing sandboxes or by establishing a sandbox jointly with the competent authorities of one or more Member States, insofar as such participation provides an equivalent level of national coverage for the participating Member States. AI sandboxes could be established in a physical, digital or hybrid form and may host both physical and digital products. Authorities creating them must also ensure that controlled AI sandboxes have adequate resources for their operation, including financial and human resources.

(139) AI sandboxes should have the objectives of boosting innovation in the field of AI by establishing a controlled experimentation and testing environment at the development and pre-commercialisation stage, with a view to ensuring that innovative AI systems comply with this Regulation and other relevant provisions of Union and national law. In addition, AI sandboxes should aim to enhance legal certainty for innovators and to support the oversight of competent authorities and their understanding of the opportunities, emerging risks and consequences of the use of AI, to facilitate regulatory learning by authorities and companies, including with a view to future adaptations of the legal framework, to support cooperation and the exchange of best practices with authorities involved in the sandbox and to accelerate market access, including by removing barriers for small and medium-sized enterprises, including start-ups. AI sandboxes should be widely available across the Union and particular attention should be paid to making them accessible to SMEs, including start-ups. Participation in the AI sandbox should focus on issues that create legal uncertainty and thus make it difficult for suppliers and potential suppliers to innovate and experiment with AI in the Union and contribute to evidence-based regulatory learning. Therefore, oversight of AI systems in the AI sandbox should cover their development, training, testing and validation before their placing on the market or putting into service, as well as the concept of "substantial modification" and its materialisation, which may necessitate a new conformity assessment procedure. Any significant risk identified during the development and testing process of these AI systems should lead to appropriate mitigation measures and, failing that, to the suspension of the development and testing process. Where appropriate, competent national authorities establishing controlled AI sandboxes should cooperate with other relevant authorities, including those overseeing the protection of fundamental rights, and may accommodate other actors in the AI ecosystem, such as national or European standardisation organisations, notified bodies, testing and experimentation facilities, research and experimentation laboratories, European digital innovation hubs and relevant stakeholder and civil society organisations. In order to ensure uniform application across the Union and achieve economies of scale,It is appropriate to establish common rules for the establishment of AI sandboxes and a framework for cooperation between relevant authorities involved in the supervision of such sandboxes. AI sandboxes established pursuant to this Regulation should be without prejudice to other legislative acts allowing the establishment of other sandboxes aimed at ensuring compliance with legislative acts other than this Regulation. Where appropriate, the relevant competent authorities in charge of those other sandboxes should weigh up the advantages of also using them for the purpose of ensuring compliance by AI systems with this Regulation. Subject to agreement between the national competent authorities and the participants in the AI sandbox, real-life testing may also be managed and supervised within the AI sandbox.

(140) This Regulation should provide the legal basis for providers and potential providers in the AI sandbox to use personal data collected for other purposes to develop certain AI systems in the public interest in the AI sandbox, only under certain conditions, in accordance with Article 6(4) and point (g) of Article 9(2) of Regulation (EU) 2016/679 and Articles 5, 6 and 10 of Regulation (EU) 2018/1725, and without prejudice to Article 4(2) and Article 10 of Directive (EU) 2016/680. The other obligations of controllers and the rights of data subjects under Regulation (EU) 2016/679, Regulation (EU) 2018/1725 and Directive (EU) 2016/680 remain applicable. In particular, this Regulation should not provide a legal basis within the meaning of Article 22(2)(b) of Regulation (EU) 2016/679 and

of Article 24(2)(b) of Regulation (EU) 2018/1725. Suppliers and potential suppliers in the controlled AI sandbox must provide appropriate safeguards and cooperate with, including by following their directions, the competent authorities and by acting swiftly and in good faith to adequately mitigate any significant risks to safety, health and fundamental rights that are identified and may arise during development, testing and experimentation in that sandbox.

(141) In order to accelerate the process of developing and placing on the market high-risk AI systems listed in an Annex to this Regulation, it is important that suppliers or potential suppliers of such systems can also benefit from a specific regime for testing such systems in real-life conditions, without participating in a controlled AI sandbox. However, in such cases, taking into account the potential consequences of such testing for natural persons, it should be ensured that the Regulation provides for adequate and sufficient safeguards and conditions for suppliers or potential suppliers. Such safeguards should include, inter alia, requesting informed consent from natural persons to participate in testing in real-life conditions, except as regards ensuring compliance with the law where attempting to obtain informed consent would prevent the testing of the AI system. The consent of subjects to participate in such testing under this Regulation is distinct from, and without prejudice to, the consent of data subjects to the processing of their personal data under relevant data protection law. It is also important to minimise risks and allow for oversight by competent authorities and therefore require potential suppliers to submit to the competent market surveillance authority a plan for the real-life test, register the test in the specific sections of the EU database, subject to some limited exceptions, set limitations on the period during which the test can be carried out and require additional safeguards for persons belonging to certain vulnerable groups, as well as a written agreement defining the roles and responsibilities of potential suppliers and those responsible for the deployment and effective oversight by competent personnel involved in the real-life test. In addition, additional safeguards should be provided to ensure that predictions, recommendations or decisions of the AI system can be effectively reversed and discarded and that personal data are protected and erased when subjects withdraw their consent to participate in the test, without prejudice to their rights as data subjects under Union data protection law. As regards the transfer of data, it is also appropriate to provide that data collected and processed for the purposes of real-life testing should only be transferred to third countries where there are appropriate and enforceable safeguards under Union law, in particular,in accordance with the bases for the transfer of personal data provided for in Union data protection law and, as regards non-personal data, there are adequate safeguards under Union law, such as Regulations (EU) 2022/868 ([42]) and (EU) 2023/2854 ([43]) of the European Parliament and of the Council.

(142) In order to ensure that AI leads to positive social and environmental outcomes, Member States are encouraged to support and promote research and development of AI solutions in support of such outcomes, such as AI-based solutions to increase accessibility for persons with disabilities, to address socio-economic inequalities or to meet environmental objectives, by allocating sufficient resources, including public and Union funds, and, where appropriate and provided that the eligibility and selection criteria are met, taking into account in particular projects pursuing such objectives. Such projects should be based on the principle of interdisciplinary cooperation between AI developers, experts in inequality and non-discrimination, accessibility and consumer rights, environmental and digital experts, as well as representatives of academia.

(143) In order to promote and protect innovation, it is important to take into particular consideration the interests of SMEs, including start-ups, which are providers or deployers of AI systems. To this end, Member States should develop awareness-raising and information communication initiatives, inter alia, targeting such operators. Member States should provide SMEs, including start-ups, which have a registered office or a branch in the Union, with priority access to AI sandboxes, provided that they meet the eligibility conditions and selection criteria and without preventing other providers and potential providers from accessing the sandboxes, provided that the same conditions and criteria are met. Member States should use existing channels and establish, where appropriate, new specific communication channels with SMEs, including start-ups, deployers, other innovators and, where appropriate, local public authorities, to support SMEs throughout their development journey by providing guidance and answering questions on the application of this Regulation. Where appropriate, these channels should work together to create synergies and ensure consistency in their guidance for SMEs, including start-ups, and deployers. In addition, Member States should encourage the involvement of SMEs and other relevant stakeholders in standardisation development processes. Notified bodies should also take into account the specific needs and interests of SMEs.

[42] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Regulation) (OJ L 152, 3.6.2022, p. 1).

[43] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules for fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Regulation) (OJ L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

providers that are SMEs, including start-ups, when setting fees for conformity assessments. The Commission should regularly assess the costs of certification and compliance for SMEs, including start-ups, through transparent consultations, and should work with Member States to reduce those costs. For example, translation costs linked to mandatory documentation and communication with authorities can be considerable for providers and other operators, in particular smaller ones. To the extent possible, Member States should ensure that one of the languages in which they accept providers to submit relevant documentation and which can be used for communication with operators is widely known by as many cross-border deployers as possible. In order to address the specific needs of SMEs, including start-ups, the Commission should provide standardised templates for the areas covered by this Regulation, upon request of the IA Council. Furthermore, the Commission should complement the efforts of the Member States by providing a single information platform with user-friendly information on this Regulation for all providers and deployers, by organising appropriate communication campaigns to raise awareness of the obligations arising from this Regulation and by assessing and promoting convergence of best practices in public procurement procedures in relation to AI systems. Medium-sized enterprises that were recently considered as small enterprises within the meaning of the Annex to Commission Recommendation 2003/361/EC [44] should have access to such support measures, as such new medium-sized enterprises may sometimes lack the legal resources and training necessary to ensure proper understanding of and compliance with this Regulation.

(144) In order to promote and protect innovation, the AI-on-demand platform and all relevant Union funding programmes and projects, such as the Digital Europe programme or Horizon Europe, implemented by the Commission and the Member States at national or Union level should, where appropriate, contribute to the achievement of the objectives of this Regulation.

(145) In order to minimise the risks to implementation resulting from a lack of market knowledge and experience, and with the aim of facilitating the fulfilment of their obligations under this Regulation by providers, in particular SMEs, including start-ups, and notified bodies, the AI-on-demand platform, the European Digital Innovation Hubs and the testing and experimentation facilities established by the Commission and the Member States at national or Union level should contribute to the implementation of this Regulation. In particular, the AI-on-demand platform, the European Digital Innovation Hubs and the testing and experimentation facilities are able to provide providers and notified bodies with technical and scientific assistance within their respective missions and areas of competence.

(146) Furthermore, in light of the very small size of some operators and in order to ensure proportionality in relation to innovation costs, it is appropriate to allow micro-enterprises to comply with one of the most costly obligations, namely to establish a quality management system, in a simplified manner, which would reduce the administrative burden and costs for such undertakings without affecting the level of protection or the need to comply with the requirements applicable to high-risk AI systems. The Commission should develop guidelines to specify the elements of the quality management system that micro-enterprises should comply with in this simplified manner.

(147) It is appropriate that the Commission should facilitate, to the extent possible, access to testing and experimental facilities to bodies, groups or laboratories established or accredited under the relevant Union harmonisation legislation and carrying out tasks within the framework of conformity assessment of products or devices covered by that legislation. This is the case, in particular, as regards expert panels, specialised laboratories and reference laboratories in the field of medical devices, in accordance with Regulations (EU) 2017/745 and (EU) 2017/746.

(148) This Regulation should establish a governance framework that allows for the coordination and support of its implementation at national level, the development of capacities at Union level and the integration of stakeholders in the field of AI. The effective implementation and enforcement of this Regulation requires a governance framework that allows for the coordination and acquisition of central expertise at Union level. The AI Office was established by Commission Decision [45] and has the mission of developing Union expertise and capacities in the field of AI and contributing to the implementation of Union law on AI. Member States should facilitate the tasks of the AI Office with a view to supporting the development of expertise and capacities at Union level and strengthening the functioning of the digital single market. In addition, an AI Board composed of representatives of the Member States, a scientific expert group to integrate the scientific community and a consultative forum should be established to facilitate stakeholder input to the implementation of this Regulation, at Union and national level. The development of expertise and capacities in the field of AI should be facilitated by the Member States.

[44] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

[45] Commission Decision of 24 January 2024 establishing the European Artificial Intelligence Office (C/2024/390).

The Union's specialised resources and capabilities should also include the use of existing resources and expertise, in particular through synergies with structures created in the context of the implementation at Union level of other legislative acts and synergies with related initiatives at Union level, such as the EuroHPC Joint Undertaking and the AI   testing and experimentation facilities under the Digital Europe programme.

(149) An AI Board should be established to facilitate the smooth, effective and harmonised implementation of this Regulation. The AI   Board should reflect the diverse interests of the AI   ecosystem and be composed of representatives of the Member States. The AI   Board should be tasked with a variety of advisory tasks. It should, inter alia, issue opinions, recommendations and advisory reports or contribute to guidance on matters related to the application of this Regulation, including as regards implementation, technical specifications or existing standards in relation to the requirements laid down in this Regulation, and advise the Commission and the Member States, as well as their national competent authorities, on specific issues related to AI. In order to provide flexibility to Member States in appointing their representatives to the AI Board, any person belonging to a public entity that has the relevant competences and powers to facilitate coordination at national level and contribute to the fulfilment of the tasks of the AI   Board may be appointed as a representative. The IA Board should establish two permanent subgroups in order to provide a platform for cooperation and exchange between market surveillance authorities and notifying authorities on issues related respectively to market surveillance and notified bodies. The permanent market surveillance subgroup should act as an administrative cooperation group (ADCO) for this Regulation within the meaning of Article 30 of Regulation (EU) 2019/1020. In accordance with Article 33 of that Regulation, the Commission should support the activities of the permanent market surveillance subgroup by carrying out market assessments or studies,
in particular with a view to identifying aspects of this Regulation that require specific and urgent coordination between market surveillance authorities. The AI   Council may establish other permanent or temporary subgroups, as appropriate, to examine specific issues. The AI   Council should also cooperate, as appropriate, with relevant Union bodies, expert groups and networks active in the context of relevant Union law, including in particular those active under relevant Union law on data and digital products and services.

(150) In order to ensure the involvement of interested parties in the implementation and application of this Regulation, an advisory forum should be established to advise the IA Board and the Commission and provide them with technical expertise. In order to ensure a diverse and balanced representation of interested parties taking into account commercial and non-commercial interests and, within the category of commercial interests, as regards the interests of the public, the IA Board and the Commission should be able to: SMEs and other businesses, the consultative forum should include, inter alia, industry, start-ups, SMEs, academia, civil society, in particular social partners, as well as the European Union Agency for Fundamental Rights, ENISA, the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications Standards Institute (ETSI).

(151) In order to support the implementation and enforcement of this Regulation, in particular the oversight activities of the AI   Office with regard to general-purpose AI models, a scientific expert group consisting of independent experts should be established. The independent experts constituting the scientific expert group should be selected on the basis of up-to-date scientific or technical knowledge in the field of AI and should perform their duties impartially and objectively and ensure the confidentiality of information and data obtained in the exercise of their duties and activities. In order to allow the reinforcement of national capacities necessary for the effective enforcement of this Regulation, Member States should be able to request the support of the experts constituting the scientific expert group for their enforcement activities.

(152) In order to support proper implementation of AI systems and to strengthen the capacities of Member States, structures supporting Union AI testing should be established and made available to Member States.

(153) Member States have a key role in the application and enforcement of this Regulation. In that regard, each Member State should designate at least one notifying authority and at least one market surveillance authority as national competent authorities responsible for overseeing its application and enforcement. Member States may decide to designate any type of public entity to carry out the tasks of national competent authorities within the meaning of this Regulation, in accordance with their specific national organisational characteristics and needs. In order to increase organisational efficiency in Member States and to establish a single official point of contact with the public and other counterparts at Member State and Union level, each Member State should designate a market surveillance authority to act as a single point of contact.

(154) The competent national authorities must exercise their powers independently, impartially and objectively, in order to preserve the principles of objectivity of their activities and functions and to ensure the application and implementation of this Regulation. Members of these authorities must refrain from any act incompatible with the nature of their functions and be subject to the rules of confidentiality laid down in this Regulation.

(155) All providers of high-risk AI systems should have a post-market surveillance system in place, with a view to ensuring that they can take into account the experience with the use of such systems in order to improve their systems and the design and development process or that they can take any corrective measures in a timely manner. Where appropriate, post-market surveillance should include an analysis of the interaction with other AI systems, including other devices andsoftware.Post-market surveillance should not cover sensitive operational data of AI system deployers who are enforcement authorities. Such a system is also essential to ensure that potential risks arising from AI systems that continue to "learn" after their introduction on the market or commissioning are addressed in a more efficient and timely manner. In this context, suppliers should also be required to have a system in place to report to the relevant authorities any serious incident associated with the use of their AI systems, understood as an incident or defect resulting in death or serious harm to health, serious and irreversible disruption to the management or operation of critical infrastructure, failure to comply with obligations under Union law intended to protect fundamental rights, or serious damage to property or the environment.

(156) In order to ensure proper and effective enforcement of the requirements and obligations provided for in this Regulation, which constitutes Union harmonisation legislation, the system relating to market surveillance and compliance of products established by Regulation (EU) 2019/1020 should be fully applied. Market surveillance authorities designated pursuant to this Regulation should have all the enforcement powers set out in this Regulation and in Regulation (EU) 2019/1020 and should exercise their powers and perform their duties in an independent, impartial and objective manner. Although most AI systems are not subject to specific requirements and obligations under this Regulation, market surveillance authorities may take measures in relation to all AI systems where they present a risk under this Regulation. Due to the specific nature of the Union institutions, bodies, offices and agencies falling within the scope of this Regulation, it is appropriate to designate the European Data Protection Supervisor as the competent market surveillance authority for them. This should be without prejudice to the designation of national competent authorities by Member States. Market surveillance activities should not affect the ability of supervised entities to carry out their tasks independently, where such independence is required by Union law.

(157) This Regulation is without prejudice to the competences, tasks, powers and independence of the relevant national public authorities or bodies overseeing the application of Union law protecting fundamental rights, including equality bodies and data protection authorities. Where necessary for their mandate, those national public authorities or bodies should also have access to any documentation created under this Regulation. A specific safeguard procedure should be laid down to ensure proper and timely enforcement against AI systems that present a risk to health, safety or fundamental rights. The procedure regarding such AI systems that present a risk should apply to high-risk AI systems that present a risk, to prohibited systems that have been placed on the market, put into service or used in contravention of the prohibited practices set out in this Regulation and to AI systems that have been placed on the market in breach of the transparency requirements set out in this Regulation and that present a risk.

(158) Union law on financial services contains rules and requirements on internal governance and risk management with which regulated financial institutions must comply when providing such services, including when using AI systems. In order to ensure the consistent application and enforcement of the obligations under this Regulation and of the relevant rules and requirements of Union legal acts relating to financial services, competent authorities to supervise and enforce those legal acts should be designated, in particular the competent authorities as defined in Regulation (EU) No 1999/2002.either575/2013 of the European Parliament and of the Council [46] and Directives 2008/48/EC [47], 2009/138/EC [48],

[46] Regulation (EU) No.either575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and amending Regulation (EU) No 575/2013.either648/2012 (OJ L 176, 27.6.2013, p. 1).

[47] Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC (OJ L 133, 22.5.2008, p. 66).

[48] Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (OJ L 335, 17.12.2009, p. 1).

2013/36/EU [49], 2014/17/EU [50] and (EU) 2016/97 [51] of the European Parliament and of the Council, within their respective competences, as the competent authorities responsible for overseeing the application of this Regulation, including as regards market surveillance activities, in relation to AI systems provided or used by regulated and supervised financial institutions, unless Member States decide to designate another authority to carry out those market surveillance tasks. Those competent authorities should have all the powers provided for in this Regulation and in Regulation (EU) 2019/1020 to enforce the requirements and obligations of this Regulation, including the powers to carry out market surveillance activities.ex postwhich may be integrated, where appropriate, into their existing supervisory mechanisms and procedures under relevant Union financial services law. It is appropriate to provide that, when acting as market surveillance authorities under this Regulation, national authorities responsible for the supervision of credit institutions regulated under Directive 2013/36/EU participating in the Single Supervisory Mechanism established by Regulation (EU) No 107/2013 shall be required to monitor the supervision of credit institutions regulated under Directive 2013/36/EU.either1024/2013 of the Council [52] communicate without delay to the European Central Bank any information obtained in the course of their market surveillance activities that may be relevant to the prudential supervision tasks of the European Central Bank specified in that Regulation. In order to enhance the coherence between this Regulation and the rules applicable to credit institutions regulated by Directive 2013/36/EU, it is also appropriate to integrate some of the procedural obligations of providers relating to risk management, post-market surveillance and documentation into the existing obligations and procedures under Directive 2013/36/EU. In order to avoid overlaps, limited exceptions should also be provided for in relation to the quality management system of providers and the surveillance obligation imposed on those responsible for the deployment of high-risk AI systems, insofar as these apply to credit institutions regulated by Directive 2013/36/EU. The same regime should apply to insurance and reinsurance undertakings and insurance holding companies regulated by Directive 2009/138/EC, to insurance intermediaries regulated by Directive (EU) 2016/97 and to other types of financial institutions subject to requirements on governance, systems or internal processes established under relevant Union financial services law in order to ensure consistency and equal treatment in the financial sector.

(159) Each market surveillance authority for high-risk AI systems in the field of biometrics listed in an Annex to this Regulation, to the extent that such systems are used for law enforcement, migration, asylum and border control management purposes, or the administration of justice and democratic processes, should have effective investigative and corrective powers, including at least the power to obtain access to all personal data being processed and all information necessary for the performance of its tasks. Market surveillance authorities should be able to exercise their powers by acting in complete independence. Any limitation on their access to sensitive operational data under this Regulation should be without prejudice to the powers conferred on them by Directive (EU) 2016/680. Any exclusion of disclosure of data to national data protection authorities under this Regulation should not affect the current or future powers of those authorities that go beyond the scope of this Regulation.

(160) Market surveillance authorities and the Commission should be able to propose joint activities, including Joint investigations, to be carried out by market surveillance authorities or market surveillance authorities together with the Commission, with the aim of promoting compliance, detecting non-compliance, raising awareness and providing guidance in relation to this Regulation with regard to specific categories of high-risk AI systems that pose a serious risk in two or more Member States. Such joint activities to promote compliance should be carried out in accordance with Article 9 of Regulation (EU) 2019/1020. The AI Office should provide coordination support to joint investigations.

(161) It is necessary to clarify the responsibilities and competences at Union and national level with regard to AI systems that are based on general-purpose AI models. In order to avoid overlapping competences, where an AI system is based on a general-purpose AI model and the model and the system are provided by the Union, the responsibilities and competences at Union and national level should be clarified.

[49] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

[50] Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1799/2008.either1093/2010 (OJ L 60, 28.2.2014, p. 34).

[51] Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on the distribution of insurance (OJ L 26, 2.2.2016, p. 19).

[52] Regulation (EU) No.either1024/2013 of the Council of 15 October 2013 conferring on the European Central Bank specific tasks concerning policies related to the prudential supervision of credit institutions (OJ L 287, 29.10.2013, p. 63).

Where the same provider is involved, oversight should be carried out at Union level through the AI Office, which should have for these purposes the powers of a market surveillance authority within the meaning of Regulation (EU) 2019/1020. In all other cases, national market surveillance authorities shall be responsible for the oversight of AI systems. However, for general-purpose AI systems that may be used directly by deployers for at least one purpose classified as high-risk, market surveillance authorities should cooperate with the AI Office to carry out conformity assessments and report thereon to the AI Council and other market surveillance authorities. In addition, market surveillance authorities should be able to request the assistance of the AI Office where the market surveillance authority is unable to conclude an investigation into a high-risk AI system due to its inability to access certain information related to the general-purpose AI model on which the high-risk AI system is based. In such cases, the following should apply:mutatis mutandisthe cross-border mutual assistance procedure provided for in Chapter VI of Regulation (EU) 2019/1020.

(162) In order to make the most of the centralisation of expertise and the resulting synergies at Union level, the powers to supervise and monitor compliance with obligations by providers of general-purpose AI models should be conferred on the Commission. The AI Office should be able to carry out all actions necessary to supervise the effective application of this Regulation as regards general-purpose AI models. It should be able to investigate potential infringements of the rules relating to providers of general-purpose AI models, both on its own initiative, following the results of its supervisory activities, and at the request of market surveillance authorities, in accordance with the conditions set out in this Regulation. In order to promote the effectiveness of supervision, the AI Office should provide for the possibility for downstream providers to submit complaints regarding potential infringements of the rules relating to providers of general-purpose AI systems and models.

(163) In order to complement the governance systems for general-purpose AI models, the Scientific Expert Group should contribute to the oversight activities of the AI Office and may, in certain cases, provide qualified alerts to the AI Office that trigger follow-up actions, such as investigations. This should be the case where the Scientific Expert Group has reason to suspect that a general-purpose AI model presents a specific and identifiable risk at Union level. This should also be the case where the Scientific Expert Group has reason to suspect that a general-purpose AI model meets the criteria that would lead to its classification as a general-purpose AI model with systemic risk. In order to provide the Scientific Expert Group with the information necessary for the performance of those tasks, a mechanism should be in place to enable the Scientific Expert Group to request documentation or information from a provider.

(164) The AI Office should be able to take the necessary measures to monitor the effective implementation and compliance with the obligations of providers of general-purpose AI models set out in this Regulation. The AI Office should be able to investigate potential infringements in accordance with the powers provided for in this Regulation, for example by requesting documentation and information, carrying out assessments and requesting measures from providers of general-purpose AI models. In carrying out the assessments, in order to be able to rely on independent expertise, the AI Office should be able to call upon independent experts to carry out the assessments on its behalf. Compliance with the obligations should be possible through, inter alia, requests for appropriate measures, including risk mitigation measures in the event of systemic risks being identified, as well as restriction of the placing on the market, withdrawal or recall of the model. As a safeguard, where necessary, in addition to the procedural rights provided for in this Regulation, providers of general-purpose AI models should have the procedural rights provided for in Article 18 of Regulation (EU) 2019/1020, which should applymutatis mutandis,without prejudice to the more specific procedural rights provided for in this Regulation.

(165) The development of AI systems other than high-risk AI systems in accordance with the requirements set out in this Regulation may lead to the broader adoption of ethical and trustworthy AI in the Union. Providers of non-high-risk AI systems should be encouraged to establish codes of conduct, including appropriate governance mechanisms, aimed at encouraging the voluntary implementation of all or part of the requirements applicable to high-risk AI systems, tailored taking into account the intended purpose of the systems and the lower risk posed and taking into account available technical solutions and industry best practices, such as model and data cards. Providers should also be encouraged and,

where appropriate, those responsible for the deployment of all AI systems, whether high-risk or not, and AI models, to apply, on a voluntary basis, additional requirements relating, for example, to the elements of the Union Ethics Guidelines for Trustworthy AI, environmental sustainability, literacy measures in

Inclusivity and diversity in the design and development of AI systems, including taking into account vulnerable persons and accessibility for persons with disabilities; stakeholder engagement, involving, as appropriate, relevant stakeholders, such as business and civil society organisations, academia, research bodies, trade unions and consumer protection organisations, in the design and development of AI systems; and diversity of development teams, including with regard to gender parity. To ensure the effectiveness of voluntary codes of conduct, they should be based on clear objectives and key performance indicators that allow the achievement of those objectives to be measured. They should also be developed in an inclusive manner, as appropriate, with the involvement of relevant stakeholders, such as business and civil society organisations, academia, research bodies, trade unions and consumer protection organisations. The Commission could formulate initiatives, including at a sectoral level, aimed at facilitating the reduction of technical barriers to cross-border data exchange for the development of AI, including in relation to data access infrastructure and the semantic and technical interoperability of different types of data.

(166) It is important that AI systems associated with products that are not considered high-risk by this Regulation and which are therefore not required to comply with the requirements set out for high-risk AI systems are, However, they are safe once placed on the market or put into service. To contribute to this objective, Regulation (EU) 2023/988 of the European Parliament and of the Council ([53]).

(167) All parties involved in the application of this Regulation should respect the confidentiality of information and data obtained by them in the performance of their duties, in accordance with Union or national law, with a view to ensuring reliable and constructive cooperation between the competent authorities at Union and national level. They should carry out their tasks and activities in a manner that protects, in particular, intellectual and industrial property rights, confidential business information and trade secrets, the effective application of this Regulation, the interests of public and national security, the integrity of criminal and administrative proceedings and the integrity of classified information.

(168) Compliance with this Regulation should be enforceable through the imposition of penalties and other enforcement measures. Member States should take all necessary measures to ensure that the provisions of this Regulation are applied, including by providing for effective, proportionate and dissuasive penalties for infringements, and to respect the principle of fairness.none other than the same.In order to strengthen and harmonise administrative penalties for infringements of this Regulation, maximum limits for the imposition of administrative fines should be set for certain specific infringements. When determining the amount of fines, Member States should take into account, in each individual case, all the relevant circumstances of the situation in question, taking into account in particular the nature, gravity and duration of the infringement and its consequences, as well as the size of the provider, in particular whether it is an SME or a start-up. The European Data Protection Supervisor should be empowered to impose fines on the Union institutions, bodies, offices and agencies falling within the scope of this Regulation.

(169) Compliance with the obligations imposed under this Regulation on providers of general-purpose AI models should be possible, inter alia, by imposing fines. To that end, fines of an appropriate amount should also be provided for in the event of non-compliance with those obligations, including failure to comply with the measures requested by the Commission pursuant to this Regulation, subject to the relevant limitation periods in accordance with the principle of proportionality. All decisions taken by the Commission pursuant to this Regulation are subject to review by the Court of Justice of the European Union in accordance with the TFEU, including the Court's unlimited jurisdiction to impose penalties pursuant to Article 261 TFEU.

(170) Union and national law already provide for effective remedies for natural and legal persons whose rights and freedoms are adversely affected by the use of AI systems. Without prejudice to those remedies, any natural or legal person who has reason to consider that an infringement of this Regulation has occurred should have the right to lodge a complaint with the relevant market surveillance authority.

(171) Affected persons should have the right to obtain an explanation where the decision of a deployer is primarily based on the output results of certain high-risk AI systems falling within the scope of this Regulation and where that decision produces legal effects.

[53] Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety and amending Regulation (EU) No 1099/2008 and Regulation (EU) No 1099/2008 and/or the European Parliament and of the Council of 10 May 2023 on general product safety and amending ...either1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and of the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (OJ L 135, 23.5.2023, p. 1).

or significantly affects such persons in a similar way, such that they consider that it has a negative effect on their health, safety or fundamental rights. Such an explanation must be clear and meaningful and serve as a basis for the affected persons to exercise their rights. The right to obtain an explanation should not apply to the use of AI systems for which exceptions or restrictions arise under Union or national law, and should only apply to the extent that this right is not already provided for by Union law.

(172) Persons reporting breaches of this Regulation should be protected by Union law. Therefore, when reporting breaches of this Regulation and as regards the protection of persons reporting such breaches, Directive (EU) 2019/1937 of the European Parliament and of the Council [54].

(173) In order to ensure that the regulatory framework can be adapted when necessary, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to amend the conditions under which an AI system should not be considered a high-risk system, the list of high-risk AI systems, the provisions relating to technical documentation, the content of the EU declaration of conformity, the provisions on conformity assessment procedures, the provisions establishing which high-risk AI systems should be subject to the conformity assessment procedure based on the assessment of the quality management system and on the assessment of the technical documentation, the threshold, benchmarks and indicators, including the possibility of supplementing those benchmarks and indicators, the rules for classifying general-purpose AI models with systemic risk, the criteria for classifying a model as a general-purpose AI model with systemic risk, the technical documentation for providers of general-purpose AI models and transparency information for providers of general-purpose AI models. It is of particular importance that the Commission carry out appropriate consultations during the preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles set out in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making [55]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(174) In view of the rapid technological developments and the know-how required for the effective implementation of this Regulation, the Commission should assess and review this Regulation by 2 August 2029 and every four years thereafter and report to the European Parliament and the Council. In addition, taking into account the implications for the scope of this Regulation, the Commission should carry out an assessment of the need to amend the list of high-risk AI systems and the list of prohibited practices once a year. In addition, by 2 August 2028 and every four years thereafter, the Commission should assess and report to the European Parliament and the Council on the need to amend the list of high-risk areas set out in the Annex to this Regulation, the AI systems falling within the scope of the transparency obligations, the effectiveness of the oversight and governance system and the progress in the development of standardisation documents on the energy-efficient development of general-purpose AI models, including the need for additional measures or actions. Finally,
By 2 August 2028 and every three years thereafter, the Commission should assess the impact and effectiveness of voluntary codes of conduct in encouraging the application of the requirements set out for high-risk AI systems to AI systems other than high-risk AI systems and possibly additional requirements for such AI systems.

(175) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 175/2009.
n.either182/2011 of the European Parliament and of the Council [56].

(176) Since the objective of this Regulation, namely to improve the functioning of the internal market and to promote the adoption of human-centred and trustworthy AI, while ensuring a high level of protection of health, safety and fundamental rights as enshrined in the Charter, including democracy, the rule of law and environmental protection, against harmful effects of AI systems in the Union, as well as supporting innovation, cannot be sufficiently achieved by the Member States but can rather, by reason of their scale and effects, be better achieved at Union level, the Union may

[54] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (OJ L 305, 26.11.2019, p. 17).

[55] OJ L 123 of 12.5.2016, p. 1.

[56] Regulation (EU) No.either182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 TEU. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(177) In order to ensure legal certainty, ensure an adequate adaptation period for operators and avoid market disruptions, including by ensuring the continued use of AI systems, it is appropriate that this Regulation should apply to high-risk AI systems that have been placed on the market or put into service before the general date of application of this Regulation only if, from that date, those systems are subject to significant changes in their design or intended purpose. It is appropriate to clarify that, In this regard, the concept of 'significant change' should be understood as being equivalent in substance to the concept of 'substantial modification', which is used only with regard to high-risk AI systems in accordance with this Regulation. As an exception and for the purposes of public accountability, operators of AI systems that are components of large-scale IT systems established by legal acts listed in an annex to this Regulation and operators of high-risk AI systems intended for use by public authorities should respectively take the necessary measures to comply with the requirements of this Regulation by the end of 2030 and by 2 August 2030.

(178) Providers of high-risk AI systems are encouraged to start complying, on a voluntary basis, with the relevant obligations of this Regulation already during the transition period.

(179) This Regulation should apply from 2 August 2026. However, taking into account the unacceptable risk associated with certain forms of use of AI, the prohibitions as well as the general provisions of this Regulation should apply as early as 2 February 2025. Although those prohibitions will not take full effect until after the establishment of governance and the application of this Regulation, it is important to anticipate the application of the prohibitions in order to take into account unacceptable risks and to accommodate other procedures, for example in the area of civil law. In addition, the infrastructure related to governance and the conformity assessment system should be operational by that date, so the provisions regarding notified bodies and the governance structure should apply from 2 August 2026. Given the rapid technological developments and the high pace of adoption of general-purpose AI models, obligations for providers of general-purpose AI models should apply from 2 August 2025. Codes of good practice should be finalised by 2 May 2025 to enable providers to demonstrate compliance with their obligations within the planned timeframe. The AI Office should ensure that the rules and classification procedures are up to date in line with technological developments. Member States should also establish and bring to the attention of the Commission rules on penalties, including administrative fines, and ensure that they are applied in an appropriate and effective manner by the date of application of this Regulation. The provisions on sanctions should therefore apply from 2 August 2025.

(180) The European Data Protection Supervisor and the European Data Protection Board, which were consulted in accordance with Article 42(1) and (2) of Regulation (EU) 2018/1725, issued their joint opinion on 18 June 2021.

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Object

1. The objective of this Regulation is to improve the functioning of the internal market and promote the uptake of human-centred and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety and fundamental rights as enshrined in the Charter, including democracy, the rule of law and environmental protection, against harmful effects of AI systems ('AI systems') in the Union and supporting innovation.

2. This Regulation provides:

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

b) prohibitions on certain AI practices;

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

(d) harmonised transparency rules applicable to certain AI systems;

(e) harmonised standards for the placing on the market of general-purpose AI models;

(f) rules on market monitoring, market surveillance, governance and compliance assurance;

g) measures to support innovation, with particular attention to SMEs, including start-ups.

Article 2

Scope of application

1. This Regulation shall apply to:

(a) providers placing on the market or putting into service AI systems or placing on the market AI models for general use in the Union, regardless of whether those providers are established or located in the Union or in a third country;

(b) those responsible for the deployment of AI systems that are established or located in the Union;

(c) providers and those responsible for deploying AI systems that are established or located in a third country, where the output results generated by the AI system are used in the Union;

d) importers and distributors of AI systems;

(e) manufacturers of products who place on the market or put into service an AI system together with their product and under their own name or brand;

(f) authorised representatives of suppliers who are not established in the Union;

(g) affected persons located in the Union.

2. For AI systems classified as high-risk AI systems in accordance with Article 6(1) and relating to products regulated by the Union harmonisation legislative acts listed in Section B of Annex I, only Article 6(1), Articles 102 to 109 and Article 112 shall apply. Article 57 shall apply only to the extent that the requirements for high-risk AI systems under this Regulation have been integrated into those Union harmonisation legislative acts.

3. This Regulation shall not apply to areas falling outside the scope of Union law and shall in any event not affect the competences of the Member States in matters of national security, regardless of the type of entity to which the Member States have entrusted the performance of tasks in relation to those competences.

This Regulation shall not apply to AI systems which, and to the extent that, are placed on the market, put into service or used, with or without modification, exclusively for military, defence or national security purposes, regardless of the type of entity carrying out these activities.

This Regulation shall not apply to AI systems that are not placed on the market or put into service in the Union where their output results are used in the Union exclusively for military, defence or national security purposes, regardless of the type of entity carrying out these activities.

4. This Regulation shall not apply to public authorities of third countries or international organisations falling within the scope of this Regulation pursuant to paragraph 1 where such authorities or organisations use AI systems in the framework of international agreements or cooperation for the purposes of law enforcement and judicial cooperation with the Union or with one or more Member States, provided that such third country or international organisation offers sufficient guarantees with regard to the protection of the fundamental rights and freedoms of individuals.

5. This Regulation shall not affect the application of the provisions relating to the liability of providers of intermediary services set out in Chapter II of Regulation (EU) 2022/2065.

6. This Regulation shall not apply to AI systems or models, including their output results, developed and put into service specifically for scientific research and development purposes only.

7. Union law on the protection of personal data, privacy and confidentiality of communications shall apply to personal data processed in relation to the rights and obligations set out in this Regulation. This Regulation shall be without prejudice to Regulations (EU) 2016/679 or (EU) 2018/1725 and Directives 2002/58/EC or (EU) 2016/680, without prejudice to Article 10(5) and Article 59 of this Regulation.

8. This Regulation shall not apply to any research, testing or development activities relating to AI systems or AI models before their placing on the market or putting into service. Those activities shall be carried out in accordance with applicable Union law. Testing in real-world conditions shall not be covered by that exclusion.

9. This Regulation shall be without prejudice to the rules laid down by other Union legal acts relating to consumer protection and product safety.

10. This Regulation shall not apply to the obligations of deployers who are natural persons using AI systems in the exercise of a purely personal, non-professional activity.

11. This Regulation shall not prevent the Union or the Member States from maintaining or introducing laws, regulations or administrative provisions which are more favourable to workers as regards the protection of their rights with regard to the use of AI systems by employers or which encourage or enable the application of collective agreements which are more favourable to workers.

12. This Regulation shall not apply to AI systems disclosed under free and open source licences, unless they are placed on the market or put into service as high-risk AI systems or as AI systems falling within the scope of Article 5 or Article 50.

Article 3

Definitions

For the purposes of this Regulation, the following definitions shall apply:

1) 'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that can exhibit adaptive capacity after deployment, and that, for explicit or implicit purposes, infers from the input information it receives how to generate output results, such as predictions, content, recommendations or decisions, that can influence physical or virtual environments;

2) 'risk' means the combination of the likelihood of harm occurring and the severity of that harm;

3) 'provider' means a natural or legal person, public authority, body, agency or agency that develops a general-purpose AI system or AI model or for which a general-purpose AI system or AI model is developed and places it on the market or puts the AI system into service under its own name or brand, whether for a fee or free of charge;

4) 'deployment controller' means a natural or legal person, public authority, body, office or agency, which uses an AI system under its own authority, except where its use is in the course of a personal, non-professional activity;

5) 'authorised representative' means a natural or legal person located or established in the Union that has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to fulfil the obligations and carry out the procedures set out in this Regulation on behalf of that provider;

6) 'importer' means a natural or legal person located or established in the Union who places on the market an AI system bearing the name or trademark of a natural or legal person established in a third country;

7) ‘distributor’ means a natural or legal person, part of the supply chain, other than the supplier or importer, who places an AI system on the Union market;

8) 'operator' means a supplier, product manufacturer, deployer, authorised representative, importer or distributor;

9) 'placing on the market' means the first placing on the Union market of an AI system or a general-purpose AI model;

10) 'placing on the market' means the supply of a general-purpose AI system or AI model for distribution or use on the Union market in the course of a commercial activity, whether for a fee or free of charge;

11) 'putting into service' means the supply of an AI system for its first use directly to the deployer or for its own use in the Union for its intended purpose;

12) 'intended purpose' means the use for which a supplier designs an AI system, including the specific context and conditions of use, as provided by the supplier in instructions for use, promotional and sales materials and statements, and 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 human behaviour or interaction with other systems, including other AI systems, that is reasonably foreseeable;

14) 'safety component' means a component of an AI product or system that performs a safety function for that AI product or system, or whose failure or malfunction endangers the health and safety of persons or property;

15) 'instructions for use' means information provided by the provider to inform the controller of the deployment, in particular, of the intended purpose and the correct use of an AI system;

16) 'recovery of an AI system' means any measure aimed at obtaining the return to the provider of an AI system made available to those responsible for the deployment, rendering it unusable or disabling its use;

17) 'withdrawal of an AI system' means any measure intended to prevent the placing on the market of an AI system that is in the supply chain;

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 establishing and carrying out the procedures necessary for the assessment, designation and notification of conformity assessment bodies and for their supervision;

20) 'conformity assessment' means the process by which it is demonstrated whether the requirements set out in Chapter III, Section 2 have been met in relation to a high-risk AI system;

21) 'conformity assessment body' means a body that carries out third-party conformity assessment activities, such as testing, certification and inspection;

22) 'notified body' means a conformity assessment body notified in accordance with this Regulation and other relevant acts of Union harmonisation legislation;

(23) 'substantial modification' means a change to an AI system after its placing on the market or putting into service that was not foreseen or planned in the initial conformity assessment carried out by the supplier and that affects the compliance of the AI system with the requirements set out in Chapter III, Section 2 or that results in a change to the intended purpose for which the AI system concerned has been assessed;

24) 'CE marking' means a marking by which a supplier indicates that an AI system complies with the requirements set out in Chapter III, Section 2, and with other applicable acts of Union harmonisation legislation providing for its placement;

(25) 'post-market surveillance' means any activities carried out by providers of AI systems aimed at collecting and examining the experience gained from the use of AI systems that they place on the market or put into service, with a view to identifying the potential need for immediate implementation of any necessary corrective or preventive measures;

26) 'market surveillance authority' means the national authority that carries out the activities and adopts the measures provided for in Regulation (EU) 2019/1020;

27) 'harmonised standard' means a harmonised standard as defined in Article 2(1)(c) of Regulation (EU) n.either1025/2012;

28) 'common specification' means a set of technical specifications as defined in Article 2(4) of Regulation (EU) No.either1025/2012 providing means to meet certain requirements laid down under this Regulation;

29) 'training data' means data used to train an AI system by adjusting its trainable parameters;

30) 'validation data' means data used to provide an evaluation of the trained AI system and to adapt its non-trainable parameters and learning process to, inter alia, avoid underfitting or overfitting;

31) 'validation data set' means an independent data set or a part of the training data set, obtained by a fixed or variable split;

32) 'test data' means data used to provide an independent assessment of the AI system, in order to confirm the intended performance of that system before it is placed on the market or put into service;

33) 'input data' means data provided to or directly obtained by an AI system from which it produces an output result;

34) 'biometric data' means personal data obtained through specific technical processing and relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data;

35) 'biometric identification' means the automated recognition of physical, physiological, behavioural or psychological characteristics of a natural person with the aim of determining the identity of a natural person by comparing his or her biometric data with biometric data of individuals held in a database;

36) 'biometric verification' means the automated one-to-one verification, including authentication, of the identity of natural persons by comparing their biometric data with biometric data previously provided;

37) ‘special categories of personal data’ means the categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725;

38) 'sensitive operational data' means operational data relating to the prevention, detection, investigation or prosecution of criminal offences, the disclosure of which could jeopardise the integrity of criminal proceedings;

39) 'emotion recognition system' means an AI system intended to distinguish or infer the emotions or intentions of natural persons from their biometric data;

40) 'biometric categorisation system' means an AI system intended to place natural persons into specific categories on the basis of their biometric data, unless it is ancillary to another commercial service and strictly necessary for objective technical reasons;

41) 'remote biometric identification system' means an AI system intended to identify natural persons without their active participation and usually remotely by comparing their biometric data with those contained in a reference database;

42) 'real-time remote biometric identification system' means a remote biometric identification system, where the collection of biometric data, comparison and identification take place without significant delay; it encompasses not only instant identification but also, in order to prevent circumvention, limited minimum delays;

43) 'delayed remote biometric identification system' means any remote biometric identification system other than a real-time remote biometric identification system;

44) 'publicly accessible space' means any physical place, whether privately or publicly owned, which can be accessed by an indeterminate number of natural persons, regardless of whether certain conditions of access must be met and regardless of any capacity restrictions;

45) "law enforcement authority":

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

(b) any other body or entity to which the law of the Member State has entrusted the exercise of 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;

46) 'law enforcement' means activities carried out by or on behalf of law enforcement authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security;

(47) ‘AI Office’ means the role of the Commission to contribute to the deployment, monitoring and oversight of AI systems and general-purpose AI models and to AI governance as provided for by the Commission Decision of 24 January 2024; references in this Regulation to the AI Office shall be construed as references to the Commission;

(48) 'national competent authority' means a notifying authority or a market surveillance authority; with regard to AI systems put into service or used by Union institutions, bodies, offices and agencies, references in this Regulation to national competent authorities or market surveillance authorities shall be construed as references to the European Data Protection Supervisor;

49) 'serious incident' means an incident or malfunction of an AI system that, directly or indirectly, results in any of the following consequences:

a) the death of a person or serious harm to his or her health;

b) a serious and irreversible disruption to the management or operation of critical infrastructure;

(c) failure to comply with obligations under Union law intended to protect fundamental rights;

d) serious damage to property or the environment;

50) 'personal data' means personal data as defined in point 1 of Article 4 of Regulation (EU) 2016/679;

51) 'non-personal data' means data other than personal data as defined in point 1 of Article 4 of Regulation (EU) 2016/679;

52) 'profiling' means profiling as defined in point (4) of Article 4 of Regulation (EU) 2016/679;

53) 'real-world test plan' means a document describing the objectives, methodology, geographical, population and temporal scope, monitoring, organisation and conduct of the real-world test;

54) 'sandbox plan' means a document agreed between the participating provider and the competent authority describing the objectives, conditions, schedule, methodology and requirements for the activities carried out in the sandbox;

(55) 'AI sandbox' means a controlled framework established by a competent authority that offers suppliers and potential suppliers of AI systems the possibility to develop, train, validate and test, under real-world conditions where appropriate, an innovative AI system, according to a sandbox plan and for a limited time, under regulatory supervision;

(56) 'AI literacy' means the skills, knowledge and understanding that enable providers, deployers and other affected persons, taking into account their respective rights and obligations in the context of this Regulation, to carry out an informed deployment of AI systems and to be aware of the opportunities and risks posed by AI, as well as the harm it may cause;

(57) ‘real-life testing’ means the temporary testing of an AI system for its intended purpose under real-life conditions, outside a laboratory or other simulation environment, in order to collect robust and reliable data and to assess and verify the compliance of the AI system with the requirements of this Regulation; if all the conditions set out in Article 57 or 60 are met, it shall not be considered as a placing on the market or putting into service of the AI system within the meaning of this Regulation;

58) 'subject' means, for the purposes of the real-life test, a natural person who participates in the real-life test;

59) 'informed consent' means the free, specific, unequivocal and voluntary expression by a subject of his or her willingness to participate in a given test under real-life conditions after having been informed of all aspects of the test that are relevant to his or her decision to participate;

60) 'deep impersonation' means image, audio or video content generated or manipulated by AI that resembles real-life persons, objects, places, entities or events and that may mislead a person into believing that they are authentic or true;

61) 'widespread infringement' means any act or omission contrary to Union law which protects the interests of individuals and which:

(a) has harmed or is likely to harm the collective interests of persons residing in at least two Member States other than that in which:

i) the act or omission originated or took place,

ii) the supplier in question or, where applicable, its authorised representative is located or established, or

iii) the person responsible for the deployment at the time of committing the infringement is established;

(b) has harmed, harms or is likely to harm the collective interests of individuals and has common characteristics – including the same unlawful practice or violation of the same interest – and is committed simultaneously by the same operator in at least three Member States;

62) ‘critical infrastructure’ means a critical infrastructure as defined in point (4) of Article 2 of Directive (EU) 2022/2557;

(63) 'general-purpose AI model' means an AI model, including one trained on a large volume of data using large-scale self-supervision, that exhibits a considerable degree of generality and is capable of competently performing a wide variety of different tasks, regardless of the way in which the model is introduced to the market, and that can be integrated into a variety of downstream systems or applications, except for AI models that are used for research, development or prototyping activities prior to being introduced to the market;

64) 'high-impact capabilities' means capabilities that match or exceed the capabilities demonstrated by the most advanced general-purpose AI models;

(65) 'systemic risk' means a risk specific to the high-impact capabilities of general-purpose AI models, which have a significant impact on the Union market due to their scope or actual or reasonably foreseeable negative effects on public health, security, public safety, fundamental rights or society as a whole, which may spread on a large scale throughout the entire value chain;

66) 'general-purpose AI system' means an AI system that is based on a general-purpose AI model and can serve a variety of purposes, both for direct use and for integration into other AI systems;

67) 'floating-point operation' means any mathematical operation or task involving floating-point numbers, which are a subset of real numbers typically represented in computers by a fixed-precision integer raised by the integer exponent of a fixed base;

68) 'downstream provider' means a provider of an AI system, including a general-purpose AI system, that integrates an AI model, regardless of whether the AI model is provided by itself and is vertically integrated or is provided by another entity under contractual relationships.

Article 4

AI Literacy

Providers and deployers of AI systems shall take measures to ensure that, to the greatest extent possible, their personnel and other persons engaged on their behalf in the operation and use of AI systems have a sufficient level of AI literacy, taking into account their technical knowledge, experience, education and training, as well as the intended context of use of the AI systems and the persons or groups of persons with whom the AI systems are to be used.

CHAPTER II

PROHIBITED AI PRACTICES

Article 5

Prohibited AI practices

1. The following AI practices are prohibited:

(a) the placing on the market, putting into service or use of an AI system that uses subliminal techniques that transcend a person's conscious awareness or deliberately manipulative or deceptive techniques with the aim or effect of substantially altering the behaviour of a person or a group of persons, thereby significantly impairing their ability to make an informed decision and causing them to make a decision that they would not otherwise have made, in a manner that causes, or is reasonably likely to cause, substantial harm to that person, another person or group of persons;

(b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a natural person or a particular group of persons arising from their age or disability, or from a particular social or economic situation, with the purpose or effect of substantially altering the behaviour of that person or a person belonging to that group in a way that causes, or is reasonably likely to cause, substantial harm to that person or another person;

(c) the placing on the market, putting into service or use of AI systems to assess or classify natural persons or groups of persons for a given period of time on the basis of their social behaviour or known, inferred or predicted personal or personality characteristics, such that the resulting citizen score results in one or more of the following situations:

(i) harmful or unfavourable treatment of certain individuals or groups of individuals in social contexts unrelated to the contexts in which the data were originally generated or collected,

(ii) harmful or unfavourable treatment of certain individuals or groups of individuals that is unjustified or disproportionate to their social behaviour or the seriousness of this behaviour;

(d) the placing on the market, putting into service for that specific purpose or use of an AI system to perform risk assessments on natural persons in order to assess or predict the risk that a natural person will commit a criminal offence based solely on the profiling of a natural person or the assessment of his or her personality traits and characteristics; this prohibition shall not apply to AI systems used to support the human assessment of a person's involvement in criminal activity which is already based on objective and verifiable facts directly related to criminal activity;

(e) the placing on the market, putting into service for this specific purpose or using AI systems that create or expand facial recognition databases by non-selective extraction of facial images from the internet or closed-circuit television;

(f) the placing on the market, putting into service for this specific purpose or using AI systems to infer the emotions of a natural person in workplaces and educational establishments, except where the AI system is intended to be installed or placed on the market for medical or security reasons;

(g) the placing on the market, putting into service for this specific purpose or use of biometric categorisation systems which individually classify natural persons on the basis of their biometric data in order to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation; this prohibition does not include the labelling or filtering of lawfully acquired biometric data sets, such as images, based on biometric data or the categorisation of biometric data in the field of law enforcement;

(h) the use of remote "real-time" biometric identification systems in public spaces for the purposes of ensuring compliance with the Law, except and to the extent that such use is strictly necessary to achieve one or more of the following objectives:

(i) the selective search for specific victims of kidnapping, human trafficking or sexual exploitation of human beings, as well as the search for missing persons,

(ii) the prevention of a specific, significant and imminent threat to the life or physical safety of natural persons or of a genuine and present or actual and foreseeable threat of a terrorist attack,

(iii) the location or identification of a person suspected of having committed an offence for the purposes of a criminal investigation or prosecution or of executing a criminal penalty for any of the offences referred to in Annex II which are punishable in the Member State concerned by a custodial sentence or detention order of a maximum duration of at least four years.

Point (h) of the first paragraph is without prejudice to Article 9 of Regulation (EU) 2016/679 concerning the processing of biometric data for purposes other than ensuring compliance with the law.

2. The use of remote "real-time" biometric identification systems in publicly accessible spaces for the purposes of ensuring compliance with the Law for any of the purposes referred to in point (h) of the first subparagraph of paragraph 1 must be deployed for the purposes set out in that point, solely to confirm the identity of the person who constitutes the specific target and shall take into account the following aspects:

(a) the nature of the situation giving rise to the possible use, and in particular the seriousness, likelihood and magnitude of the harm that would result if the system were not used;

(b) the consequences that the use of the system would have on the rights and freedoms of the persons concerned, and in particular the seriousness, likelihood and magnitude of those consequences.

Furthermore, the use of remote "real-time" biometric identification systems in publicly accessible spaces for enforcement purposes for any of the purposes referred to in point (h) of the first subparagraph of paragraph 1 of this Article shall comply with necessary and proportionate safeguards and conditions relating to the use in accordance with national law authorising such use, in particular as regards temporal, geographical and personal limitations. The use of remote "real-time" biometric identification systems in publicly accessible spaces shall only be authorised if the enforcement authority has completed a fundamental rights impact assessment as provided for in Article 27 and has registered the system in the EU database in accordance with Article 49. However, in duly justified cases of urgency, the use of such systems may be started without registration in the EU database, provided that such registration is completed without undue delay.

3. For the purposes of point (h) of the first subparagraph of paragraph 1 and paragraph 2, any use of a "real-time" remote biometric identification system in publicly accessible spaces for enforcement purposes shall be subject to prior authorisation by a judicial authority or an independent administrative authority whose decision is binding on the Member State in which the system is to be used, which shall be issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 5. However, in a duly justified situation of urgency, the use of such a system may be started without authorisation provided that such authorisation is requested without undue delay but not later than within 24 hours. If such authorisation is refused, the use shall be discontinued with immediate effect and all data, as well as results and output information generated by such use, shall be discarded and deleted immediately.

The competent judicial authority or an independent administrative authority whose decision is binding shall only grant authorisation if it is satisfied, on the basis of objective evidence or clear indications put to it, that the use of the "real-time" remote biometric identification system is necessary and proportionate in order to achieve one of the objectives specified in point (h) of the first subparagraph of paragraph 1, which shall be indicated in the application, and in particular is limited to what is strictly necessary as regards the period of time and the geographical and personal scope. When making its decision, that authority shall take into account the aspects referred to in paragraph 2. Such authorisation shall be limited to the period of time and the geographical and personal scope of the application.

The authority may not adopt any decision that produces adverse legal effects for a person solely on the basis of the output results of the remote biometric identification system "in real time".

4. Without prejudice to paragraph 3, any use of a "real-time" remote biometric identification system in publicly accessible spaces for enforcement purposes shall be notified to the relevant market surveillance authority and to the national data protection authority in accordance with the national rules referred to in paragraph 5. The notification shall contain, as a minimum, the information specified in paragraph 6 and shall not include sensitive operational data.

5. Member States may decide to provide for the possibility of authorising, in whole or in part, the use of remote "real-time" biometric identification systems in publicly accessible spaces for enforcement purposes within the limits and under the conditions set out in point (h) of the first subparagraph of paragraph 1 and paragraphs 2 and 3. The Member States concerned shall lay down in their national law the necessary detailed rules applicable to the application, granting and exercise of the authorisations referred to in paragraph 3, as well as to the monitoring and reporting in relation thereto. Those rules shall also specify for which purposes among those listed in point (h) of the first subparagraph of paragraph 1, and, where appropriate, in relation to which offences among those listed in point (h)(iii), competent authorities may be authorised to use such systems for enforcement purposes. Member States shall notify those rules to the Commission not later than 30 days after their adoption. Member States may, in accordance with Union law, adopt more restrictive laws on the use of remote biometric identification systems.

6. National market surveillance authorities and national data protection authorities of Member States that have been notified of the use of remote "real-time" biometric identification systems in publicly accessible spaces for enforcement purposes pursuant to paragraph 4 shall submit annual reports to the Commission on such use. To this end, the Commission shall provide Member States and national market surveillance and data protection authorities with a template containing information on the number of decisions taken by competent judicial authorities or an independent administrative authority whose decision is binding on applications for authorisation pursuant to paragraph 3 and their outcome.

7. The Commission shall publish annual reports on the use of remote 'real-time' biometric identification systems in publicly accessible spaces for enforcement purposes prepared on the basis of aggregated data relating to Member States on the basis of the annual reports referred to in paragraph 6. Those annual reports shall not include sensitive operational data of the related enforcement activities.

8. This Article shall not affect prohibitions applicable where an AI practice infringes other provisions of Union law.

CHAPTER III

HIGH RISK AI SYSTEMS

SECTION 1

Classification of AI systems as high-risk systems

Article 6

Classification rules for high-risk AI systems

1. Irrespective of whether it has been placed on the market or put into service without being integrated into the products referred to in points (a) and (b), an AI system shall be considered high-risk when it meets both of the following conditions:

(a) the AI system is intended to be used as a security component of a product falling within the scope of the Union harmonisation legislative acts listed in Annex I, or the AI system itself is one of such products, and

(b) the product of which the AI system is a safety component pursuant to point (a), or the AI system itself as a product, must undergo a third-party conformity assessment for its placing on the market or putting into service in accordance with the Union harmonisation legislative acts listed in Annex I.

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.

3. Notwithstanding paragraph 2, an AI system referred to in Annex III shall not be considered high-risk if it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not substantially influencing the outcome of decision-making.

The first paragraph shall apply when any of the following conditions are met:

a) the AI system is intended to perform a limited procedural task;

b) that the AI system is intended to improve the result of a previously performed human activity;

(c) the AI system is intended to detect patterns of decision-making or deviations from previous patterns of decision-making and is not intended to replace or influence previously made human judgment without appropriate human review, or

(d) the AI system is intended to perform a preparatory task for an assessment that is relevant for the purposes of the use cases listed in Annex III.

Notwithstanding the first paragraph, AI systems referred to in Annex III shall always be considered high-risk when the AI system profiles natural persons.

4. A provider that considers that an AI system referred to in Annex III is not high-risk shall document its assessment before that system is placed on the market or put into service. That provider shall be subject to the registration obligation set out in Article 49(2). At the request of the competent national authorities, the provider shall provide documentation of the assessment.

5. The Commission shall, after consulting the European Artificial Intelligence Council ('AI Council'), by 2 February 2026, provide guidelines specifying the practical application of this Article in line with Article 96, together with an exhaustive list of practical examples of high-risk and non-high-risk AI systems use cases.

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 97 to amend the second subparagraph of paragraph 3 of this Article by adding new conditions to or amending those set out in that paragraph where there is concrete and reliable evidence of the existence of AI systems falling within the scope of Annex III but which do not pose a significant risk of harm to the health, safety or fundamental rights of natural persons.

7. The Commission shall adopt delegated acts in accordance with Article 97 to amend the second subparagraph of paragraph 3 of this Article by deleting any of the conditions laid down therein, where there is specific and reliable evidence that this is necessary in order to maintain the level of protection of health, safety and fundamental rights provided for in this Regulation.

8. No modification to the conditions laid down in the second subparagraph of paragraph 3 adopted in accordance with paragraphs 6 and 7 of this Article shall reduce the overall level of protection of health, safety and fundamental rights provided for in this Regulation, and any modification shall ensure consistency with the delegated acts adopted pursuant to Article 7(1) and take into account technological and market developments.

Article 7

Amendments to Annex III

1. The Commission shall be empowered to adopt delegated acts in accordance with Article 97 to amend Annex III by adding or modifying use cases for high-risk AI systems where both of the following conditions are met:

(a) the AI systems are intended for use in any of the areas listed in Annex III, and

(b) the AI systems pose a risk of harm to health and safety or negative impacts on fundamental rights, and that risk is equivalent to or greater than the risk of harm or negative impacts posed by high-risk AI systems already mentioned in Annex III.

2. When assessing the condition referred to in paragraph 1(b), 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 or is likely to be used;

(c) the nature and amount of the data processed and used by the AI system, in particular where special categories of personal data are processed;

(d) the degree of autonomy with which the AI system acts and the possibility for a human to override a decision or recommendation that may result in harm;

(e) the extent to which the use of an AI system has already caused harm to health and safety, had negative impacts on fundamental rights or given rise to significant concerns regarding the likelihood of such harm or negative impacts, as demonstrated, for example, by documented reports or allegations submitted to competent national authorities or any other reports, as appropriate;

(f) the potential extent of such harm or negative impact, in particular as regards its intensity and its potential to affect several persons or to disproportionately affect a particular group of persons;

(g) the extent to which the persons who might suffer such harm or such negative impacts depend on the result generated by an AI system, in particular because it is not reasonably possible for practical or legal reasons to opt out of such a result;

(h) the extent to which there is an imbalance of power or the persons who could suffer such harm or negative impact are in a position of vulnerability in relation to the person responsible for deploying an AI system, in particular due to their situation, authority, knowledge, economic or social circumstances, or age;

(i) the extent to which the result generated using an AI system is easily corrected or reversed, taking into account the technical solutions available to correct or reverse it and without results that adversely affect health, safety or fundamental rights being considered as easy to correct or reverse;

(j) the likelihood that the deployment of the AI system will result in benefits for individuals, communities or society at large, and the magnitude of this benefit, including potential improvements in product safety;

(k) the extent to which applicable Union law provides for:

(i) effective remedies in relation to the risks posed by an AI system, excluding actions for damages,

(ii) effective measures to prevent or significantly reduce such risks.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 97 to amend the list in Annex III by deleting high-risk AI systems where both of the following conditions are met:

(a) the high-risk AI systems concerned no longer pose significant risks to fundamental rights, health or safety, taking into account the criteria listed in paragraph 2;

(b) the deletion does not reduce the general level of protection of health, safety and fundamental rights under Union law.

SECTION 2

Requirements for high-risk AI systems

Article 8

Compliance with requirements

1. High-risk AI systems shall comply with the requirements set out in this Section, taking into account their intended purposes as well as the generally recognised state of the art in AI and AI-related technologies. When ensuring compliance with those requirements, account shall be taken of the risk management system referred to in Article 9.

2. Where a product contains an AI system to which the requirements of this Regulation apply as well as the requirements of the Union legislative acts on harmonisation listed in Section A of Annex I, suppliers shall be responsible for ensuring that their product fully complies with all applicable requirements under the applicable Union legislative acts on harmonisation. In order to ensure compliance of high-risk AI systems referred to in paragraph 1 with the requirements set out in this Section, and in order to ensure consistency, avoid duplication and minimise additional burdens, suppliers may choose to integrate, as appropriate, the necessary testing and reporting processes, and the information and documentation they provide in respect of their product into existing documentation and procedures required by the Union legislative acts on harmonisation listed in Section A of Annex I.

Article 9

Risk management system

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

2. The risk management system shall be understood as a continuous iterative process planned and executed throughout the life cycle of a high-risk AI system, which shall require periodic systematic reviews and updates. It shall consist of the following stages:

(a) the determination and analysis of the known and foreseeable risks that the high-risk AI system may pose to health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose;

(b) the estimation and assessment of the risks that could arise when the high-risk AI system is used in accordance with its intended purpose and when it is subject to reasonably foreseeable misuse;

(c) the assessment of other risks that could arise from the analysis of the data collected through the post-market surveillance system referred to in Article 72;

(d) the adoption of appropriate and specific risk management measures designed to address the risks identified in accordance with point (a).

3. The risks referred to in this Article are only those that can be reasonably mitigated or eliminated by the development or design of the high-risk AI system or the provision of appropriate technical information.

4. The risk management measures referred to in point (d) of paragraph 2 shall take due account of the effects and potential interaction arising from the combined application of the requirements set out in this Section, with a view to minimising risks most effectively while achieving an appropriate balance in the application of measures to meet those requirements.

5. The risk management measures referred to in point (d) of paragraph 2 shall consider the relevant residual risks associated with each hazard as acceptable, as well as the overall residual risk of high-risk AI systems.

When determining the most appropriate risk management measures, the following will be sought:

(a) eliminate or reduce the risks identified and assessed in accordance with paragraph 2 to the extent technically feasible through appropriate design and development of the high-risk AI system;

b) implement, where appropriate, appropriate mitigation and control measures to address risks that cannot be eliminated;

(c) provide the information required in accordance with Article 13 and, where appropriate, provide training to those responsible for deployment.

With a view to eliminating or reducing the risks associated with the use of the high-risk AI system, due consideration shall be given to the technical knowledge, experience, education and training expected of the deployer, as well as the context in which the system is intended to be used.

6. High-risk AI systems shall be subject to testing to determine the most appropriate and specific risk management measures. Such testing shall verify that high-risk AI systems operate in a manner consistent with their intended purpose and comply with the requirements set out in this Section.

7. Test procedures may include tests under real conditions in accordance with Article 60.

8. Testing of high-risk AI systems shall be carried out, as appropriate, at any point during the development process and, in any case, before their introduction to the market or commissioning. Testing shall be carried out using pre-defined parameters and probability thresholds that are appropriate for the intended purpose of the high-risk AI system.

9. When implementing the risk management system provided for in paragraphs 1 to 7, providers shall pay attention to whether, in view of its intended purpose, the high-risk AI system is likely to adversely affect persons under the age of eighteen and, where applicable, other vulnerable groups.

10. In the case of providers of high-risk AI systems that are subject to requirements relating to internal risk management processes under other relevant provisions of Union law, the aspects provided for in paragraphs 1 to 9 may be part of, or combined with, the risk management procedures established under that law.

Article 10

Data and data governance

1. High-risk AI systems using techniques involving training AI models with data shall be developed using training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5 whenever such data sets are used.

2. Training, validation and testing data sets shall be subject to data governance and management practices appropriate to the intended purpose of the high-risk AI system. Such practices shall focus in particular on the following:

a) relevant design decisions;

b) the data collection processes and the origin of the data and, in the case of personal data, the original purpose of the data collection;

c) the processing operations necessary for the preparation of the data, such as annotation, labelling, cleansing, updating, enrichment and aggregation;

d) the formulation of assumptions, in particular with regard to the information that the data are supposed to measure and represent;

e) an assessment of the availability, quantity and adequacy of the data sets needed;

(f) the examination of any biases that may affect the health and safety of persons, adversely affect fundamental rights or give rise to any form of discrimination prohibited by Union law, in particular where data outputs influence the inputs of future transactions;

(g) appropriate measures to detect, prevent and mitigate potential biases detected in accordance with point (f);

(h) the identification of relevant gaps or deficiencies in the data that impede compliance with this Regulation, and how to remedy them.

3. Training, validation and test data sets shall be relevant, sufficiently representative and, to the greatest extent possible, free from errors and complete in view of their intended purpose. They shall also have appropriate statistical properties, for example, where relevant, with respect to the persons or groups of persons in relation to whom the high-risk AI system is intended to be used. Data sets may have those characteristics for each data set individually or for a combination of data sets.

4. The data sets shall take into account, to the extent necessary for the intended purpose, the particular characteristics or elements of the specific geographical, contextual, behavioural or functional environment in which the high-risk AI system is intended to be used.

5. To the extent strictly necessary to ensure the detection and correction of biases associated with high-risk AI systems in accordance with points (f) and (g) of paragraph 2 of this Article, providers of such systems may exceptionally process special categories of personal data provided that they provide appropriate safeguards in relation to the fundamental rights and freedoms of natural persons. In addition to the provisions set out in Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680, for such processing to take place, all of the following conditions must be met:

a) that the processing of other data, such as synthetic or anonymised data, does not allow for effective detection and correction of biases;

(b) that special categories of personal data are subject to technical limitations on the reuse of personal data and to state-of-the-art security and privacy protection measures, including pseudonymisation;

(c) that special categories of personal data are subject to measures to ensure that the personal data processed are secured, protected and subject to appropriate safeguards, including strict controls and documentation of access, in order to prevent misuse and ensure that only authorised persons have access to such personal data with appropriate confidentiality obligations;

(d) that special categories of personal data are not transmitted or transferred to third parties and that they cannot otherwise have access to them;

(e) that special categories of personal data be deleted once the bias has been corrected or the personal data have reached the end of their retention period, whichever is earlier;

(f) records of processing activities pursuant to Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680 include the reasons why the processing of special categories of personal data was strictly necessary to detect and correct bias and why that objective could not be achieved by the processing of other data.

6. For the development of high-risk AI systems that do not employ techniques involving the training of AI models, paragraphs 2 to 5 shall apply only to test data sets.

Article 11

Technical documentation

1. The technical documentation of a high-risk AI system shall be developed before its introduction on the market or commissioning, and shall be kept up to date.

The technical documentation shall be drawn up in such a way as to demonstrate that the high-risk AI system complies with the requirements set out in this Section and to provide, in a clear and complete manner, the national competent authorities and notified bodies with the information necessary to assess the conformity of the AI system with those requirements. It shall contain, as a minimum, the elements referred to in Annex IV. SMEs, including start-ups, may provide the elements of the technical documentation specified in Annex IV in a simplified manner. For this purpose, the Commission shall establish a simplified form for technical documentation geared to the needs of small and micro enterprises. Where an SME, including a start-up, chooses to provide the information required by Annex IV in a simplified manner, it shall use the form referred to in this paragraph. That form shall be accepted by notified bodies for the purposes of conformity assessment.

2. Where a high-risk AI system associated with a product falling within the scope of the Union harmonisation legislative acts referred to in Section A of Annex I is placed on the market or put into service, a single set of technical documents shall be drawn up containing all the information referred to in paragraph 1 as well as the information required by those legislative acts.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 97 to amend Annex IV, where necessary, to ensure that, in view of technical developments, the technical documentation provides all the information necessary to assess whether the system complies with the requirements set out in this Section.

Article 12

Record keeping

1. High-risk AI systems shall technically enable the automatic recording of events (hereinafter "log files") throughout the entire life cycle of the system.

2. To ensure a level of traceability of the operation of the high-risk AI system that is appropriate for the intended purpose of the system, logging capabilities shall allow for the recording of events relevant to:

(a) the detection of situations that may lead to the high-risk AI system presenting a risk within the meaning of Article 79(1) or to a substantial modification;

(b) the facilitation of post-market surveillance referred to in Article 72, and

(c) the monitoring of the operation of high-risk AI systems referred to in Article 26(5).

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

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

b) the reference database against which the system has compared the input data;

c) the input data to which the search has yielded a match;

(d) the identification of the natural persons involved in the verification of the results referred to in Article 14, paragraph 5.

Article 13

Transparency and communication of information to those responsible for deployment

1. High-risk AI systems shall be designed and developed in a way that ensures that they operate with a level of transparency sufficient for deployers to correctly interpret and use their output results. An appropriate type and level of transparency shall be ensured to enable the provider and the deployer to comply with the relevant obligations under Section 3.

2. High-risk AI systems shall be accompanied by relevant instructions for use in a digital or other suitable format, which shall include concise, complete, correct and clear information that is relevant, accessible and understandable to those responsible for deployment.

3. The instructions for use shall contain at least the following information:

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

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

i) its intended purpose,

(ii) the level of accuracy (including parameters for measuring it), robustness and cybersecurity referred to in Article 15 with respect to which the high-risk AI system has been tested and validated and which can be expected, as well as any known and foreseeable circumstances that may affect the expected level of accuracy, robustness and cybersecurity,

(iii) any known or foreseeable circumstances associated with the use of the high-risk AI system in accordance with its intended purpose or with reasonably foreseeable misuse, which may give rise to risks to health and safety or fundamental rights referred to in Article 9(2);

(iv) where applicable, the capabilities and technical characteristics of the high-risk AI system to provide relevant information to explain its output results,

(v) where applicable, its operation in relation to certain persons or certain groups of persons in relation to whom the system is intended to be used,

(vi) where applicable, specifications regarding the input data, or any other relevant information regarding the training, validation and testing data sets used, taking into account the intended purpose of the high-risk AI system,

(vii) where applicable, information that enables those responsible for the deployment to interpret the output results of the high-risk AI system and to use it appropriately;

(c) changes to the high-risk AI system and its operation predetermined by the supplier at the time of the initial conformity assessment, if applicable;

(d) the human oversight measures referred to in Article 14, including technical measures established to facilitate the interpretation of the output results of high-risk AI systems by those responsible for deployment;

(e) the necessary computing and hardware resources, the expected lifetime of the high-risk AI system and the necessary maintenance and care measures (including their frequency) to ensure the proper functioning of such system, including with regard to updates to the system.software;

(f) where applicable, a description of the mechanisms included in the high-risk AI system that allow those responsible for the deployment to correctly collect, store and interpret log files in accordance with Article 12.

Article 14

Human supervision

1. High-risk AI systems shall be designed and developed so that they can be effectively monitored by natural persons during the period they are in use, including by providing them with appropriate human-machine interface tools.

2. The objective of human oversight shall be to prevent or minimise risks to health, safety or fundamental rights that may arise when a high-risk AI system is used in accordance with its intended purpose or when it is subject to reasonably foreseeable misuse, in particular where such risks persist despite the application of other requirements set out in this Section.

3. The supervisory measures shall be proportionate to the risks, level of autonomy and context of use of the high-risk AI system, and shall be ensured either by one of the following types of measures, or by both:

(a) measures that the provider defines and integrates, where technically feasible, into the high-risk AI system prior to its introduction on the market or its putting into service;

(b) measures that the provider defines prior to the high-risk AI system being placed on the market or put into service and that are suitable for implementation by the deployer.

4. For the purposes of implementing paragraphs 1, 2 and 3, the high-risk AI system shall be offered to the deployer in such a way that natural persons entrusted with human supervision may, as appropriate and in a manner proportionate to:

(a) adequately understand the relevant capabilities and limitations of the high-risk AI system and be able to appropriately monitor its operation, for example, with a view to detecting and resolving anomalies, malfunctions and unexpected behaviour;

(b) be aware of the potential tendency to automatically or over-rely on the output results generated by a high-risk AI system ("automation bias"), in particular with those systems that are used to provide information or recommendations for the purpose of decision-making by natural persons;

c) correctly interpret the output results of the high-risk AI system, taking into account, for example, the available interpretation methods and tools;

d) decide, in any specific situation, not to use the high-risk AI system or to discard, invalidate or reverse the output results it generates;

e) intervene in the operation of the high-risk AI system or interrupt the system by pressing a stop button or using a similar procedure that allows the system to be stopped safely.

5. In the case of high-risk AI systems referred to in point (a) of Annex III, point 1, the measures referred to in paragraph 3 of this Article shall also ensure that the deployer does not act or take any decision based on the identification generated by the system, unless that identification has been separately verified and confirmed by at least two natural persons with the necessary competence, training and authority.

The requirement for verification by at least two separate natural persons shall not apply to high-risk AI systems used for law enforcement, migration, border control or asylum purposes where the application of this requirement is deemed disproportionate under Union or national law.

Article 15

Accuracy, robustness and cybersecurity

1. High-risk AI systems shall be designed and developed to achieve an appropriate level of accuracy, robustness and cybersecurity and to perform consistently in these respects throughout their lifecycle.

2. In order to address technical aspects of how to measure the appropriate levels of accuracy and robustness set out in paragraph 1 and any other relevant performance parameters, the Commission, in cooperation with relevant stakeholders and organisations, such as metrology and benchmarking authorities, shall, as appropriate, promote the development of reference parameters and measurement methodologies.

3. The instructions for use accompanying high-risk AI systems shall indicate the accuracy levels of such systems, as well as the relevant parameters for measuring their accuracy.

4. High-risk AI systems shall be as resilient as possible with regard to errors, failures or inconsistencies that may arise in the systems themselves or in the environment in which they operate, in particular as a result of their interaction with natural persons or other systems. Technical and organisational measures shall be taken in this regard.

Robustness of high-risk AI systems can be achieved through technical redundancy solutions, such as backups or failover plans.

High-risk AI systems that continue to learn after their introduction to the market or commissioning shall be developed in such a way as to eliminate or reduce as far as possible the risk that potentially biased output results influence the input information for future operations (feedback loops) and to ensure that such loops are adequately addressed by appropriate risk mitigation measures.

5. High-risk AI systems will be resistant to attempts by unauthorized third parties to alter their use, output results, or operation by exploiting vulnerabilities in the system.

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

Technical solutions to address specific AI vulnerabilities will include, as appropriate, measures to prevent, detect, combat, resolve and control attacks that attempt to manipulate the training data set ("data poisoning"), or pre-trained components used in training ("model poisoning"), input information designed to cause the AI model to make an error ("adversarial examples" or "model evasion"), confidentiality attacks or defects in the model.

SECTION 3

Obligations of suppliers and those responsible for deploying high-risk AI systems and other parties

Article 16

Obligations of providers of high-risk AI systems

High-risk AI system providers:

(a) ensure that their high-risk AI systems comply with the requirements defined in Section 2;

(b) indicate on the high-risk AI system or, where this is not possible, on the system packaging or accompanying documentation, as applicable, their name, registered trade name or trademark and their contact address;

(c) have a quality management system that complies with the provisions of Article 17;

(d) retain the documentation referred to in Article 18;

(e) where under their control, retain log files automatically generated by their high-risk AI systems referred to in Article 19;

(f) ensure that high-risk AI systems are subject to the relevant conformity assessment procedure referred to in Article 43 before they are placed on the market or put into service;

(g) draw up an EU declaration of conformity in accordance with Article 47;

(h) affix the CE marking to the high-risk AI system or, where this is not possible, to its packaging or accompanying documentation, to indicate compliance with this Regulation, in accordance with Article 48;

(i) comply with the registration obligations referred to in Article 49(1);

(j) take the necessary corrective measures and provide the information required in Article 20;

(k) demonstrate, upon reasoned request of the competent national authority, the compliance of the high-risk AI system with the requirements set out in Section 2;

(l) ensure that the high-risk AI system complies with accessibility requirements in accordance with Directives (EU) 2016/2102 and (EU) 2019/882.

Article 17

Quality management system

1. Providers of high-risk AI systems shall establish a quality management system to ensure compliance with this Regulation. That system shall be systematically and orderly documented in documentation containing policies, procedures and instructions and shall include at least the following aspects:

(a) a strategy for compliance with the regulations, including compliance with conformity assessment procedures and procedures for managing modifications to high-risk AI systems;

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

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

(d) the review, testing and validation procedures that will be carried out before, during and after the development of the high-risk AI system, as well as the frequency with which they will be executed;

(e) the technical specifications, including standards, to be applied and, where the relevant harmonised standards do not apply in full or do not cover all the relevant requirements set out in Section 2, the means to be used to ensure that the high-risk AI system complies with those requirements;

(f) data management systems and procedures, including their acquisition, collection, analysis, labelling, storage, filtering, prospecting, aggregation, retention and any other data-related operations carried out prior to and for the placing on the market or commissioning of high-risk AI systems;

g) the risk management system referred to in Article 9;

(h) the establishment, implementation and maintenance of a post-market surveillance system in accordance with Article 72;

(i) the procedures associated with the notification of a serious incident pursuant to Article 73;

(j) managing communication with competent national authorities, other relevant authorities, including those granting or facilitating access to data, notified bodies, other operators, customers or other interested parties;

k) systems and procedures for keeping records of all relevant documentation and information;

l) resource management, including measures related to security of supply;

(m) an accountability framework that defines the responsibilities of management and other staff in relation to all aspects listed in this section.

2. The application of the aspects referred to in paragraph 1 shall be proportionate to the size of the provider's organisation. Providers shall, in any case, respect the degree of rigour and level of protection required to ensure the compliance of their high-risk AI systems with this Regulation.

3. Providers of high-risk AI systems that are subject to obligations relating to quality management systems or an equivalent function under relevant sectoral Union law may include the aspects listed in paragraph 1 as part of the quality management systems under that law.

4. For providers that are financial institutions subject to requirements relating to their governance, systems or internal processes under Union financial services law, the obligation to establish a quality management system shall be deemed to have been fulfilled, except in relation to points (g), (h) and (i) of paragraph 1 of this Article, where the rules on internal governance systems or processes under the relevant Union financial services law are respected. For this purpose, all harmonised rules referred to in Article 40 shall be taken into account.

Article 18

Conservation of documentation

1. For a period of ten years from the placing on the market or putting into service of the high-risk AI system, the provider shall keep at the disposal of the competent national authorities:

a) the technical documentation referred to in Article 11;

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

c) documentation relating to changes approved by notified bodies, if applicable;

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

(e) the EU declaration of conformity referred to in Article 47.

2. Each Member State shall determine the conditions under which the documentation referred to in paragraph 1 shall remain at the disposal of the competent national authorities during the period referred to in that paragraph in cases where a supplier or his authorised representative established in its territory goes bankrupt or ceases to operate before the end of that period.

3. Providers that are financial institutions subject to requirements relating to their governance, systems or internal processes under Union financial services law shall maintain the technical documentation as part of the documentation maintained under the relevant Union financial services law.

Article 19

Automatically generated log files

1. Providers of high-risk AI systems shall retain log files referred to in Article 12(1) that are automatically generated by high-risk AI systems to the extent that such files are under their control. Without prejudice to applicable Union or national law, log files shall be retained for a period of time appropriate to the intended purpose of the high-risk AI system, at least six months, unless otherwise provided by applicable Union or national law, in particular Union law on the protection of personal data.

2. Providers that are financial institutions subject to requirements relating to their governance, systems or internal processes under Union financial services law shall maintain log files automatically generated by their high-risk AI systems as part of the documentation maintained under the relevant financial services law.

Article 20

Corrective measures and reporting obligations

1. Suppliers of high-risk AI systems that consider or have reason to consider that a high-risk AI system that they have placed on the market or put into service is not in compliance with this Regulation shall immediately take the necessary corrective measures to bring it into compliance, to withdraw it from the market, deactivate it or recall it, as appropriate. They shall inform the distributors of the high-risk AI system concerned and, where applicable, those responsible for the deployment, the authorised representative and the importers thereof.

2. Where a high-risk AI system presents a risk within the meaning of Article 79(1) and the provider is aware of that risk, the provider shall immediately investigate the causes, in collaboration with the deployer who notified the system, where applicable, and inform the market surveillance authorities competent for the high-risk AI system concerned and, where applicable, the notified body that has issued a certificate for that system in accordance with Article 44, in particular of the nature of the non-compliance and any corrective measures taken.

Article 21

Cooperation with competent authorities

1. Providers of high-risk AI systems shall, upon a reasoned request from a competent authority, provide that authority with all information and documentation necessary to demonstrate the compliance of the high-risk AI system with the requirements set out in Section 2, in a language that is easily understood by the authority and which is one of the official languages of the Union institutions, as indicated by the Member State concerned.

2. Upon a reasoned request from a competent authority, providers shall also give that authority, where appropriate, access to the automatically generated log files of the high-risk AI system referred to in Article 12(1), insofar as those files are under their control.

3. Any information obtained by a competent authority pursuant to this Article shall be treated in accordance with the confidentiality obligations set out in Article 78.

Article 22

Authorized representatives of high-risk AI system providers

1. Before placing their high-risk AI systems on the Union market, providers established in third countries shall appoint, by means of a written mandate, an authorised representative who is established in the Union.

2. Suppliers shall allow their authorized representative to carry out the tasks specified in the mandate received from the supplier.

3. Authorised representatives shall carry out the tasks specified in the mandate received from the supplier. They shall provide the market surveillance authorities, upon request, with a copy of the mandate in one of the official languages of the Union institutions as indicated by the competent authority. For the purposes of this Regulation, the mandate shall enable the authorised representative to carry out the following tasks:

(a) verify that the EU declaration of conformity referred to in Article 47 and the technical documentation referred to in Article 11 have been drawn up and that the supplier has carried out an appropriate conformity assessment procedure;

(b) keep at the disposal of the competent authorities and the national authorities or bodies referred to in Article 74(10) for a period of 10 years from the placing on the market or putting into service of the high-risk AI system, the contact details of the provider who appointed the authorised representative, a copy of the EU declaration of conformity referred to in Article 47, the technical documentation and, where applicable, the certificate issued by the notified body;

(c) provide a competent authority, upon reasoned request, with all information and documentation, including that referred to in point (b) of this paragraph, necessary to demonstrate the compliance of a high-risk AI system with the requirements set out in Section 2, including access to the log files referred to in Article 12(1) automatically generated by that system, insofar as those files are under the control of the provider;

(d) cooperate with the competent authorities, upon reasoned request, in all actions undertaken by them in relation to the high-risk AI system, in particular to reduce and mitigate the risks it presents;

(e) where applicable, comply with the registration obligations referred to in Article 49(1) or, where registration is carried out by the provider itself, ensure that the information referred to in Section A, point 3 of Annex VIII is correct.

The mandate shall enable the authorised representative to be contacted by the competent authorities, in addition to the supplier or instead of the supplier, with reference to all matters relating to ensuring compliance with this Regulation.

4. The authorised representative shall terminate the mandate if it considers or has reason to consider that the supplier is in breach of its obligations under this Regulation. In such a case, it shall also immediately inform the relevant market surveillance authority and, where applicable, the relevant notified body of the termination of the mandate and the reasons for this measure.

Article 23

Obligations of importers

1. Before placing a high-risk AI system on the market, importers shall ensure that the system complies with this Regulation by verifying that:

(a) the provider of the high-risk AI system has carried out the relevant conformity assessment procedure referred to in Article 43;

(b) the supplier has drawn up the technical documentation in accordance with Article 11 and Annex IV;

(c) the system bears the required CE marking and is accompanied by the EU declaration of conformity referred to in Article 47 and the instructions for use;

(d) the supplier has appointed an authorised representative in accordance with Article 22(1).

2. Where the importer has reasonable grounds to consider that a high-risk AI system is not in compliance with this Regulation, has been falsified or is accompanied by falsified documentation, the importer shall not place the system on the market until compliance has been achieved for that system. Where the high-risk AI system presents a risk within the meaning of Article 79(1), the importer shall inform the provider of the system, authorised representatives and market surveillance authorities thereof.

3. Importers shall indicate, on the packaging of the high-risk AI system or in the accompanying documentation, where applicable, their name, registered trade name or trademark and their contact address.

4. While responsible for a high-risk AI system, importers shall ensure that the conditions of storage or transport, where applicable, do not compromise the compliance of that system with the requirements set out in Section 2.

5. Importers shall retain, for a period of ten years from the time the high-risk AI system is placed on the market or put into service, a copy of the certificate issued by the notified body, where applicable, containing the instructions for use and the EU declaration of conformity referred to in Article 47.

6. Importers shall provide the relevant competent authorities, upon reasoned request, with all information and documentation, including those referred to in paragraph 5, necessary to demonstrate the compliance of a high-risk AI system with the requirements set out in Section 2 in a language easily understood by those authorities. To this end, they shall also ensure that the technical documentation can be made available to those authorities.

7. Importers shall cooperate with the relevant competent authorities in any measures taken by them in relation to a high-risk AI system placed on the market by importers, in particular to reduce and mitigate the risks presented by it.

Article 24

Obligations of distributors

1. Before placing a high-risk AI system on the market, distributors shall verify that it bears the required CE marking, that it is accompanied by a copy of the EU declaration of conformity referred to in Article 47 and the instructions for use, and that the supplier and importer of that system, as applicable, have complied with their obligations under Article 16(b) and (c) and Article 23(3), respectively.

2. If a distributor considers or has reason to consider, based on the information in its possession, that a high-risk AI system does not comply with the requirements set out in Section 2, it shall not place the system on the market until such compliance has been achieved. In addition, if the high-risk AI system presents a risk within the meaning of Article 79(1), the distributor shall inform the supplier or importer of the system, as appropriate.

3. While responsible for a high-risk AI system, distributors shall ensure that storage or transport conditions, where applicable, do not compromise the system's compliance with the requirements set out in Section 2.

4. Distributors who consider, or have reason to consider, on the basis of the information in their possession, that a high-risk AI system that they have placed on the market is not in compliance with the requirements set out in Section 2 shall take the necessary corrective measures to bring it into compliance, to withdraw it from the market or to recall it, or shall ensure that the supplier, importer or other relevant operator, as appropriate, takes such corrective measures. Where a high-risk AI system presents a risk within the meaning of Article 79(1), its distributor shall immediately inform the supplier or importer of the system and the competent authorities in respect of the high-risk AI system concerned, giving details, in particular, of the non-compliance and any corrective measures taken.

5. Upon a reasoned request from a relevant competent authority, distributors of a high-risk AI system shall provide that authority with all information and documentation relating to their actions under paragraphs 1 to 4 that are necessary to demonstrate that the system complies with the requirements set out in Section 2.

6. Distributors shall cooperate with the relevant competent authorities in any measures they take in relation to a high-risk AI system placed on the market by the distributors, in particular to reduce or mitigate the risks it presents.

Article 25

Responsibilities across the AI value chain

1. Any distributor, importer, deployer or third party shall be considered a provider of a high-risk AI system for the purposes of this Regulation and shall be subject to the provider obligations set out in Article 16 in any of the following circumstances:

(a) where it puts its name or trademark on a high-risk AI system previously placed on the market or put into service, without prejudice to contractual arrangements stipulating that obligations are otherwise allocated;

(b) where it substantially modifies a high-risk AI system that has already been placed on the market or put into service in such a way that it remains a high-risk AI system pursuant to Article 6;

(c) where it modifies the intended purpose of an AI system, including a general-purpose AI system, which has not been identified as high-risk and has already been placed on the market or put into service, such that the AI system concerned becomes a high-risk AI system in accordance with Article 6.

2. Where the circumstances referred to in paragraph 1 apply, the supplier that initially placed the AI system on the market or put it into service shall no longer be considered as a supplier of that specific AI system for the purposes of this Regulation. That initial supplier shall cooperate closely with new suppliers and provide reasonably foreseeable necessary information, technical access or other assistance necessary for the fulfilment of the obligations set out in this Regulation, in particular with regard to compliance with the conformity assessment of high-risk AI systems. This paragraph shall not apply in cases where the initial supplier has clearly indicated that its AI system should not be transformed into a high-risk AI system and is therefore not subject to the obligation to provide documentation.

3. In the case of high-risk AI systems that are security components of products covered by the Union harmonisation legislative acts listed in Section A of Annex I, the manufacturer of the product shall be considered as a provider of the high-risk AI system and shall be subject to the obligations provided for in Article 16 in one of the following circumstances:

(a) the high-risk AI system is placed on the market together with the product under the name or brand of the manufacturer of the product;

b) the high-risk AI system is put into service under the name or brand of the product manufacturer after the product has been introduced to the market.

4. The provider of a high-risk AI system and the third party supplying a high-risk AI system, tools, services, components or processes to be used or integrated into a high-risk AI system shall specify, by written agreement, the information, capabilities, technical access and other assistance that are necessary, on the basis of generally recognised state of the art, to enable the provider of the high-risk AI system to fully comply with the obligations set out in this Regulation. This paragraph shall not apply to third parties that make publicly available tools, services, processes or components other than general-purpose AI models, under a free and open source licence.

The AI Office may develop and recommend voluntary standard contractual clauses between providers of high-risk AI systems and third parties that provide tools, services, components or processes that are used or integrated into high-risk AI systems. When developing such voluntary standard contractual clauses, the AI Office shall take into account potential contractual requirements applicable in particular sectors or business models. The voluntary standard contractual clauses shall be published and made freely available in an easily usable electronic format.

5. Paragraphs 2 and 3 shall be without prejudice to the need to observe and protect intellectual and industrial property rights, confidential business information and trade secrets in accordance with Union and national law.

Article 26

Obligations of those responsible for the deployment of high-risk AI systems

1. Those responsible for deploying high-risk AI systems shall take appropriate technical and organisational measures to ensure that they use such systems in accordance with the accompanying instructions for use, in accordance with paragraphs 3 and 6.

2. Those responsible for deployment shall entrust human supervision to natural persons who have the necessary competence, training and authority.

3. The obligations laid down in paragraphs 1 and 2 shall not affect any other obligations imposed on those responsible for the deployment by Union or national law or their freedom to organise their own resources and activities in order to implement the human oversight measures indicated by the provider.

4. Without prejudice to paragraphs 1 and 2, the deployer shall ensure that the input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system, to the extent that it exercises control over such input data.

5. Deployers shall monitor the operation of the high-risk AI system based on the instructions for use and, where appropriate, inform suppliers in accordance with Article 72. Where deployers have reason to consider that using the high-risk AI system in accordance with their instructions may result in that AI system posing a risk within the meaning of Article 79(1), they shall, without undue delay, inform the supplier or distributor and the relevant market surveillance authority and suspend the use of that system. Where deployers detect a serious incident, they shall also immediately report that incident first to the supplier and then to the importer or distributor and the relevant market surveillance authority. In the event that the deployer is unable to contact the supplier, Article 73 shall apply.mutatis mutandis.This obligation shall not cover sensitive operational data of those responsible for deploying AI systems who are authorities responsible for ensuring compliance with the law.

In the case of deployers that are financial institutions subject to requirements relating to their governance, systems or internal processes under Union financial services law, the oversight obligation provided for in the first subparagraph shall be deemed to have been fulfilled where the rules on internal governance systems, processes and arrangements in accordance with the relevant Union financial services law are respected.

6. Controllers deploying high-risk AI systems shall retain log files automatically generated by high-risk AI systems to the extent that such files are under their control, for a period of time appropriate to the intended purpose of the high-risk AI system, at least six months, unless otherwise provided for by applicable Union or national law, in particular Union law on the protection of personal data.

Deployment controllers that are financial institutions subject to requirements relating to their governance, systems or internal processes under Union financial services law shall maintain the log files as part of the documentation maintained under Union financial services law.

7. Before deploying or using a high-risk AI system in the workplace, deployers who are employers shall inform workers' representatives and affected workers that they will be exposed to the use of the high-risk AI system. This information shall be provided, where appropriate, in accordance with the rules and procedures laid down in Union and national law and in accordance with practices regarding information to workers and their representatives.

8. Those responsible for the deployment of high-risk AI systems that are public authorities or Union institutions, bodies, offices and agencies shall comply with the registration obligations referred to in Article 49. Where those deployers find that the high-risk AI system they intend to use has not been registered in the EU database referred to in Article 71, they shall not use that system and shall inform the supplier or distributor.

9. Where applicable, controllers deploying high-risk AI systems shall use the information provided pursuant to Article 13 of this Regulation to comply with their obligation to carry out a data protection impact assessment pursuant to Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680.

10. Notwithstanding Directive (EU) 2016/680, in the context of an investigation the purpose of which is the selective search for a person suspected of or convicted of having committed a crime, the person responsible for deploying a high-risk AI system for remote biometric identification in a deferred manner shall request,ex anteor without undue delay and not later than within forty-eight hours, to a judicial or administrative authority whose decisions are binding and subject to judicial review, an authorization to use such a system, except when it is used for the initial identification of a possible suspect on the basis of objective and verifiable facts directly related to the offence. Any such use shall be limited to what is strictly necessary for the investigation of a particular offence.

In the event that the authorisation provided for in the first paragraph is denied, the remote biometric identification system that is the subject of the authorisation request will cease to be used with immediate effect and the personal data associated with the use of the high-risk AI system for which the authorisation was requested will be deleted.

Such a high-risk AI system for remote deferred biometric identification shall in no case be used for the purposes of ensuring compliance with the Law in an indiscriminate manner, without any connection to a crime, a criminal proceeding, a real and present or real and foreseeable threat of crime, or to the search for a specific missing person. It shall be ensured that law enforcement authorities cannot take any decision that produces adverse legal effects for a person solely on the basis of the output results of such remote deferred biometric identification systems.

This section is without prejudice to Article 9 of Regulation (EU) 2016/679 and Article 10 of Directive (EU) 2016/680 for the processing of biometric data.

Regardless of the purpose or the person responsible for the deployment, any use of such high-risk AI systems shall be documented in the relevant law enforcement file and made available upon request to the relevant market surveillance authority and the national data protection authority, excluding the disclosure of sensitive operational data related to enforcement. This paragraph shall be without prejudice to the powers conferred by Directive (EU) 2016/680 on supervisory authorities.

Deployers shall submit annual reports to the relevant market surveillance authority and the national data protection authority on their use of remote biometric identification systems, excluding disclosure of sensitive operational data related to enforcement. Reports may be aggregated to cover more than one deployment.

Member States may, in accordance with Union law, adopt more restrictive laws on the use of remote and delayed biometric identification systems.

11. Without prejudice to Article 50 of this Regulation, controllers responsible for the deployment of high-risk AI systems referred to in Annex III that take decisions or assist in taking decisions relating to natural persons shall inform natural persons that they are exposed to the use of high-risk AI systems. For high-risk AI systems used for enforcement purposes, Article 13 of Directive (EU) 2016/680 shall apply.

12. Deployers shall cooperate with the relevant competent authorities in any measures they take in relation to the high-risk AI system for the purpose of implementing this Regulation.

Article 27

Fundamental rights impact assessment for high-risk AI systems

1. Before deploying a high-risk AI system referred to in Article 6(2), with the exception of high-risk AI systems intended for use in the field listed in point 2 of Annex III, deployers that are bodies governed by public law, or private entities providing public services, and those responsible for the deployment of high-risk AI systems referred to in points (b) and (c) of point 5 of Annex III, shall carry out an assessment of the impact that the use of those systems may have on fundamental rights. To that end, deployers shall carry out an assessment consisting of:

(a) a description of the deployer's processes in which the high-risk AI system will be used in accordance with its intended purpose;

b) a description of the period of time over which each high-risk AI system is expected to be used and the frequency with which it is expected to be used;

c) the categories of natural persons and groups that may be affected by its use in the specific context;

(d) the specific risks of harm that may affect the categories of natural persons and groups determined in accordance with point (c) of this paragraph, taking into account the information provided by the supplier in accordance with Article 13;

e) a description of the application of human monitoring measures, in accordance with the instructions for use;

(f) the measures to be taken in the event that such risks materialise, including internal governance arrangements and grievance mechanisms.

2. The obligation described in paragraph 1 shall apply to the first use of the high-risk AI system. In similar cases, the deployer may rely on previously conducted fundamental rights impact assessments or on existing impact assessments conducted by providers. If, during the use of the high-risk AI system, the deployer considers that any of the elements listed in paragraph 1 have changed or are no longer up-to-date, the deployer shall take the necessary measures to update the information.

3. Once the assessment referred to in paragraph 1 of this Article has been carried out, the person responsible for the deployment shall notify the market surveillance authority of its results by submitting the completed form referred to in paragraph 5 of this Article. In the case referred to in Article 46(1), the persons responsible for the deployment may be exempted from this notification obligation.

4. If any of the obligations set out in this Article are already fulfilled by the data protection impact assessment carried out pursuant to Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, the fundamental rights impact assessment referred to in paragraph 1 of this Article shall complement that data protection impact assessment.

5. The AI Office shall develop a model questionnaire, including through an automated tool, to facilitate deployers to fulfil their obligations under this Article in a simplified manner.

SECTION 4

Notifying authorities and notified bodies

Article 28

Notifying authorities

1. Each Member State shall appoint or establish at least one notifying authority which shall be responsible for establishing and carrying out the procedures necessary for the assessment, designation and notification of conformity assessment bodies, as well as for their supervision. These procedures shall be developed through cooperation between the notifying authorities of all Member States.

2. Member States may decide that the assessment and supervision referred to in paragraph 1 will be carried out by a national accreditation body within the meaning of Regulation (EC) No.$_{\text{either}}$765/2008 and in accordance with this.

3. Notifying authorities shall be constituted, organised and operate in such a way that no conflict of interest arises with conformity assessment bodies and that the impartiality and objectivity of their activities is ensured.

4. Notifying authorities shall be organised in such a way that decisions concerning the notification of conformity assessment bodies are taken by competent persons other than those who carried out the assessment of those bodies.

5. Notifying authorities shall not offer or carry out any activities carried out by conformity assessment bodies, nor any consultancy services of a commercial or competitive nature.

6. The notifying authorities shall maintain the confidentiality of the information obtained, in accordance with the provisions of Article 78.

7. Notifying authorities shall have sufficient competent staff to carry out their tasks properly. Where appropriate, competent staff shall have the necessary expertise to perform their tasks, in areas such as information technology, AI and law, including the monitoring of fundamental rights.

Article 29

Request for notification by a conformity assessment body

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 request for notification shall be accompanied by a description of the conformity assessment activities, the conformity assessment module(s) and the types of AI systems for which the conformity assessment body considers itself competent, as well as a certificate of accreditation, if any, issued by a national accreditation body, declaring that the conformity assessment body complies with the requirements set out in Article 31.

Any valid documents relating to existing designations of the applicant notified body under any other act of Union harmonisation legislation shall be added.

3. If the conformity assessment body concerned is unable to provide an accreditation certificate, it shall provide the notifying authority with all documentary evidence necessary to verify, recognise and periodically monitor its compliance with the requirements set out in Article 31.

4. As regards notified bodies designated in accordance with any other Union harmonisation legislation, all documents and certificates linked to such designations may be used to support their designation procedure under this Regulation, as appropriate. The notified body shall update the documentation referred to in paragraphs 2 and 3 of this Article when relevant changes occur, in order to enable the authority responsible for notified bodies to monitor and verify that all the requirements set out in Article 31 continue to be met.

Article 30

Notification procedure

1. Notifying authorities may only notify conformity assessment bodies that have complied with the requirements laid down in Article 31.

2. The notifying authorities shall notify the Commission and the other Member States, by means of the electronic notification system developed and managed by the Commission, of each conformity assessment body referred to in paragraph 1.

3. The notification referred to in paragraph 2 of this Article shall include detailed information on the conformity assessment activities, the conformity assessment module(s) and the types of AI systems concerned, as well as the relevant certification of competence. Where the notification is not based on the accreditation certificate referred to in Article 29(2), the notifying authority shall provide the Commission and the other Member States with documentary evidence demonstrating the competence of the conformity assessment body and the arrangements in place to ensure that the body is regularly monitored and continues to satisfy the requirements set out in Article 31.

4. The conformity assessment body concerned may only carry out the activities of a notified body if no objection is raised by the Commission or by other Member States within two weeks of notification by a notifying authority where the latter includes the accreditation certificate referred to in Article 29(2) or two months of notification by the notifying authority where the latter includes the documentary evidence referred to in Article 29(3).

5. Where objections are raised, the Commission shall without delay enter into consultations with the relevant Member States and the conformity assessment body. In the light of these, the Commission shall forward its decision to the Member State concerned and to the relevant conformity assessment body.

Article 31

Requirements for notified bodies

1. Notified bodies shall be established in accordance with the national law of the Member States and shall have legal personality.

2. Notified bodies shall meet the organisational, quality management, resource and process requirements necessary for the performance of their functions, as well as appropriate cybersecurity requirements.

3. The organisational structure, distribution of responsibilities, reporting lines and functioning of notified bodies shall provide confidence in their performance and in the results of the conformity assessment activities carried out by the notified bodies.

4. Notified bodies shall be independent of the provider of a high-risk AI system in relation to which they carry out conformity assessment activities. Notified bodies shall be independent of any other operator with an economic interest in the high-risk AI systems being assessed, as well as of any competitor of the provider. This shall not preclude the use of assessed high-risk AI systems that are necessary for the activities of the conformity assessment body or the use of such high-risk systems for personal purposes.

5. Conformity assessment bodies, their top management and personnel responsible for carrying out conformity assessment tasks shall not be directly involved in the design, development, marketing or use of such high-risk AI systems, nor shall they represent the parties carrying out these activities. Furthermore, they shall not carry out any activity that might conflict with their independence of judgement or integrity in relation to the conformity assessment activities for which they have been notified. This shall apply in particular to consultancy services.

6. Notified bodies shall be organised and managed in such a way as to ensure the independence, objectivity and impartiality of their activities. Notified bodies shall document and implement a structure and procedures which ensure impartiality and enable the principles of impartiality to be promoted and put into practice throughout their organisation, to all their staff and in all their assessment activities.

7. Notified bodies shall have documented procedures ensuring that their staff, committees, subsidiaries, subcontractors and any associated bodies or staff of external bodies maintain, in accordance with Article 78, the confidentiality of information coming into their possession in the performance of conformity assessment activities, except in cases where disclosure is required by law. The staff of notified bodies shall be bound by professional secrecy in respect of all information obtained in the performance of their tasks under this Regulation, except in relation to the notifying authorities of the Member State in which they carry out their activities.

8. Notified bodies shall have procedures in place for carrying out their activities which take due account of the size of the providers, the sector in which they operate, their structure and the degree of complexity of the AI system concerned.

9. Notified bodies shall take out appropriate liability insurance for their conformity assessment activities, unless liability is assumed by the Member State in which they are established under national law or the Member State itself is directly responsible for the conformity assessment.

10. Notified bodies shall be capable of carrying out all their tasks under this Regulation with the highest degree of professional integrity and the necessary technical competence in the specific field, whether such tasks are carried out by the notified bodies themselves or on their behalf and under their responsibility.

11. Notified bodies shall have sufficient internal technical competence to be able to effectively assess tasks carried out on their behalf by external actors. The notified body shall permanently have sufficient administrative, technical, legal and scientific staff with experience and knowledge of the relevant types of AI systems, data and data computing and the requirements set out in Section 2.

12. Notified bodies shall participate in coordination activities as provided for in Article 38. They shall also take part directly or through representation in European standardisation organisations, or shall ensure that they are kept abreast of the current status of the relevant standards.

Article 32

Presumption of conformity with the requirements relating to notified bodies

Where a conformity assessment body demonstrates compliance with the criteria set out in the relevant harmonised standards, or parts thereof, the references of which are published in theOfficial Journal of the European Union,It shall be presumed to comply with the requirements set out in Article 31 to the extent that the applicable harmonised standards provide for those same requirements.

Article 33

Subsidiaries of notified bodies and subcontracting

1. Where a notified body subcontracts specific tasks related to conformity assessment or uses a subsidiary, it shall ensure that the subcontractor or subsidiary complies with the requirements set out in Article 31 and shall inform the notifying authority accordingly.

2. Notified bodies shall assume full responsibility for the tasks carried out by any subcontractors or subsidiaries.

3. Activities may only be subcontracted or delegated to a subsidiary with the prior consent of the supplier. Notified bodies shall make a list of their subsidiaries publicly available.

4. Relevant documents concerning the assessment of the qualifications of the subcontractor or subsidiary and the work carried out by them under this Regulation shall be kept at the disposal of the notifying authority for a period of five years from the date of completion of the subcontracting.

Article 34

Operational obligations of notified bodies

1. Notified bodies shall verify the conformity of high-risk AI systems following the conformity assessment procedures set out in Article 43.

2. Notified bodies shall avoid unnecessary burdens for providers when carrying out their activities and shall take due account of the size of the provider, the sector in which it operates, its structure and the degree of complexity of the high-risk AI system concerned, in particular with a view to minimising administrative burdens and costs of compliance for micro and small enterprises within the meaning of Recommendation 2003/361/EC. The notified body shall, however, respect the degree of stringency and the level of protection required for the high-risk AI system to comply with the requirements of this Regulation.

3. Notified bodies shall make available to the notifying authority referred to in Article 28, and shall submit to it upon request, all relevant documentation, including documentation of suppliers, in order to enable the notifying authority referred to in Article 28 to carry out its assessment, designation, notification and monitoring activities and to facilitate the assessment described in this Section.

Article 35

Identification numbers and lists of notified bodies

1. The Commission shall assign a unique identification number to each notified body, even where a body is notified under more than one Union act.

2. The Commission shall make public the list of bodies notified under this Regulation, including their identification numbers and the activities for which they have been notified. The Commission shall ensure that the list is kept up to date.

Article 36

Changes in notifications

1. The notifying authority shall notify the Commission and the other Member States of any relevant changes to the notification of a notified body by means of the electronic notification system referred to in Article 30(2).

2. The procedures laid down in Articles 29 and 30 shall apply to extensions of the scope of the notification.

For modifications to the notification other than extensions of its scope, the procedures set out in paragraphs 3 to 9 shall apply.

3. Where a notified body decides to terminate its conformity assessment activities, it shall inform the notifying authority and the suppliers concerned as soon as possible and, in the case of a planned cessation, at least one year before it terminates its activities. The certificates of the notified body may remain valid for a period of nine months after the cessation of the notified body's activities, provided that another notified body has confirmed in writing that it will assume responsibility for the high-risk AI systems covered by those certificates. That latter notified body shall carry out a full assessment of the high-risk AI systems concerned before the expiry of that nine-month period and before issuing new certificates for those systems. Where the notified body has terminated its activities, the notifying authority shall withdraw the designation.

4. Where a notifying authority has reasonable grounds to consider that a notified body no longer complies with the requirements set out in Article 31 or is not fulfilling its obligations, the notifying authority shall investigate the matter without delay and with the utmost diligence. In that context, it shall inform the notified body concerned of the objections raised and give it the opportunity to present its views. Where the notifying authority concludes that the notified body no longer complies with the requirements set out in Article 31 or is not fulfilling its obligations, it shall limit, suspend or withdraw the designation, as appropriate, depending on the seriousness of the failure to comply with those requirements or obligations. It shall also immediately inform the Commission and the other Member States thereof.

5. Where its designation has been suspended, restricted or withdrawn in whole or in part, the notified body shall inform the affected suppliers within ten days.

6. In the event of limitation, suspension or withdrawal of a designation, the notifying authority shall take appropriate measures to ensure that the files of the notified body concerned are retained and to make them available to notifying authorities of other Member States and to market surveillance authorities upon request.

7. In the event of limitation, suspension or withdrawal of a designation, the notifying authority shall:

(a) assess the impact on the certificates issued by the notified body;

(b) submit to the Commission and the other Member States a report containing its findings within three months of notification of the changes in the designation;

(c) require the notified body to suspend or withdraw, within a reasonable period determined by the authority, any certificates improperly issued, in order to ensure the continued conformity of high-risk AI systems on the market;

(d) shall inform the Commission and the Member States of the certificates whose suspension or withdrawal it has requested;

(e) provide the competent national authorities of the Member State in which the supplier has its registered office with all relevant information concerning the certificates whose suspension or withdrawal it has requested; that authority shall take appropriate measures, where necessary, to prevent a risk to health, safety or fundamental rights.

8. Except in the case of certificates issued improperly, and where a designation has been suspended or limited, certificates shall remain valid under one of the following circumstances:

(a) where, within one month of the suspension or limitation, the notifying authority has confirmed that there is no risk to health, safety or fundamental rights in relation to the certificates affected by the suspension or limitation and has set out a timetable for action to remedy the suspension or limitation, or

(b) where the notifying authority has confirmed that no certificates related to the suspension will be issued, amended or reissued for the duration of the suspension or limitation and declares whether or not the notified body has the capacity, during the period of the suspension or limitation, to continue to monitor and be responsible for the certificates issued; where the notifying authority determines that the notified body does not have the capacity to support the certificates issued, the provider of the system covered by the certificate shall confirm in writing to the competent national authorities of the Member State in which it has its registered office, within three months of the suspension or limitation, that another qualified notified body will temporarily take over the functions of the notified body in monitoring and being responsible for the certificates during the period of the suspension or limitation.

9. Except in the case of certificates issued improperly, and where a designation has been withdrawn, certificates shall remain valid for nine months in the following circumstances:

(a) the competent national authority of the Member State in which the provider of the high-risk AI system covered by the certificate has its registered office has confirmed that there is no risk to health, safety or fundamental rights associated with the high-risk AI system in question, and

b) another notified body has confirmed in writing that it will assume immediate responsibility for such AI systems and completes its assessment within twelve months of the withdrawal of the designation.

In the circumstances referred to in the first paragraph, the competent national authority of the Member State in which the provider of the system covered by the certificate has its registered office may extend the provisional validity of the certificates for additional periods of three months, without exceeding twelve months in total.

The competent national authority or the notified body assuming the functions of the notified body affected by the change of designation shall immediately inform the Commission, the other Member States and the other notified bodies.

Article 37

Questioning the competence of notified bodies

1. The Commission shall, where necessary, investigate any cases where there are reasons to doubt the competence of a notified body or the continued compliance by a notified body with the requirements set out in Article 31 and its applicable responsibilities.

2. The notifying authority shall, upon request, provide the Commission with all relevant information relating to the notification or the maintenance of competence of the notified body concerned.

3. The Commission shall ensure confidential treatment in accordance with Article 78 of all sensitive information collected in the course of its investigations under this Article.

4. Where the Commission determines that a notified body does not or no longer complies with the requirements for its notification, it shall inform the notifying Member State accordingly and request it to take the necessary corrective measures, including the suspension or withdrawal of the designation where necessary. Where the Member State does not take the necessary corrective measures, the Commission may, by means of an implementing act, suspend, restrict or withdraw the designation. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 98(2).

Article 38

Coordination of notified bodies

1. The Commission shall ensure that appropriate coordination and cooperation between notified bodies active in conformity assessment procedures under this Regulation, in the form of a sectoral group of notified bodies, is established and maintained in relation to high-risk AI systems.

2. Each notifying authority shall ensure that the bodies notified by it participate in the work of the group referred to in paragraph 1, directly or through designated representatives.

3. The Commission shall arrange for exchanges of knowledge and best practices to be organised between notifying authorities.

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, provided that they comply with the requirements set out in Article 31 or ensure an equivalent level of compliance.

SECTION 5

Standards, conformity assessment, certificates, registration

Article 40

Harmonized standards and standardization documents

1. High-risk AI systems or general-purpose AI models that comply with harmonized standards, or parts thereof, whose references are published in theOfficial Journal of the European Unionin accordance with Regulation (EU) No. either1025/2012 shall be presumed to comply with the requirements set out in Section 2 of this Chapter or, where applicable, with the obligations set out in Chapter V, Sections 2 and 3 of this Regulation, to the extent that those rules provide for these requirements or obligations.

2. In accordance with Article 10 of Regulation (EU) No.either1025/2012, the Commission shall, without undue delay, make requests for standardisation covering all the requirements set out in Section 2 of this Chapter and, where appropriate, requests for standardisation covering the obligations set out in Sections 2 and 3 of Chapter V of this Regulation. The request for standardisation shall also include a request for documents on processes for submitting information and documentation in order to improve the resource-efficient performance of AI systems, such as reducing the energy and other resource consumption of high-risk AI systems during their life cycle, as well as on the energy-efficient development of general-purpose AI models. When preparing a request for standardisation, the Commission shall consult the AI Council and relevant stakeholders, including the Consultative Forum.

When addressing a request for standardisation to the European standardisation organisations, the Commission shall specify that the standards should be clear, consistent – including with standards developed in various sectors for products covered by the existing Union harmonisation legislative acts listed in Annex I – and aimed at ensuring that high-risk AI systems or general-purpose AI models placed on the market or put into service in the Union comply with the relevant requirements or obligations set out in this Regulation.

The Commission shall request the European standardisation organisations to provide evidence that they have made every effort to meet the objectives referred to in the first and second subparagraphs of this paragraph, in accordance with Article 24 of Regulation (EU) No 1999/2003.either1025/2012.

3. Participants in the standardisation process shall seek to promote investment and innovation in AI, including by increasing legal certainty as well as the competitiveness and growth of the Union market, to contribute to the strengthening of global cooperation in favour of standardisation, taking into account existing international standards in the field of AI that are consistent with the values, fundamental rights and interests of the Union, and to enhance multilateral governance, ensuring a balanced representation of interests and effective participation of all relevant stakeholders in accordance with Articles 5, 6 and 7 of Regulation (EU) No 1999/2002.either1025/2012.

Article 41

Common specifications

1. The Commission may adopt implementing acts laying down common specifications for the requirements set out in Section 2 of this Chapter or, as appropriate, for the obligations set out in Chapter V, Sections 2 and 3, provided that the following conditions have been met:

(a) the Commission has requested, pursuant to Article 10(1) of Regulation (EU) No.either1025/2012, to one or more European standardisation organisations to develop a harmonised standard for the requirements set out in Section 2 of this Chapter, or as appropriate, for the obligations set out in Chapter V, Sections 2 and 3, and:

i) the application has not been accepted by any of the European standardisation organisations, or

(ii) the harmonised standards responding to that request have not been delivered within the period laid down in accordance with Article 10(1) of Regulation (EU) No.either1025/2012, or

(iii) the relevant harmonised standards do not sufficiently address fundamental rights concerns, or

iv) the harmonised standards do not correspond to the request, and

b) has not been published in theOfficial Journal of the European Unionno reference to harmonised standards governing the requirements set out in Section 2 of this Chapter, or as applicable, the obligations referred to in Chapter V, Sections 2 and 3, in accordance with Regulation (EU) No.either1025/2012 and the publication of such reference is not expected within a reasonable period.

When drawing up common provisions, the Commission shall consult the consultative forum referred to in Article 67.

The implementing acts referred to in the first subparagraph of this paragraph shall be adopted in accordance with the examination procedure referred to in Article 98(2).

2. Before drawing up a draft implementing act, the Commission shall inform the committee referred to in Article 22 of Regulation (EU) No 1799/2003.either1025/2012, which considers that the conditions set out in section 1 of this article have been met.

3. High-risk AI systems or general-purpose AI models that comply with the common specifications referred to in paragraph 1, or parts of those specifications, shall be presumed to comply with the requirements set out in Section 2 of this Chapter or, as applicable, for the purposes of complying with the obligations referred to in Chapter V, Sections 2 and 3, to the extent that those common specifications address those requirements or those obligations.

4. When a harmonised standard is adopted by a European standardisation organisation and proposed to the Commission for the purpose of publishing its reference in theOfficial Journal of the European Union,The Commission will assess the harmonised standard in accordance with Regulation (EU) No.either1025/2012. When the reference to a harmonised standard is published in theOfficial Journal of the European Union,The Commission shall repeal the implementing acts referred to in paragraph 1, or parts of those acts, which provide for the same requirements set out in Section 2 of this Chapter or, as appropriate, the same obligations set out in Chapter V, Sections 2 and 3.

5. Where providers of high-risk AI systems or general-purpose AI models do not comply with the common specifications referred to in paragraph 1, they shall duly justify that they have adopted technical solutions that comply with the requirements referred to in Section 2 of this Chapter or, as applicable, comply with the obligations set out in Chapter V, Sections 2 and 3, at a level at least equivalent to those.

6. Where a Member State considers that a common specification does not fully comply with the requirements set out in Section 2, or, as applicable, does not comply with the obligations set out in Chapter V, Sections 2 and 3, it shall inform the Commission thereof with a detailed explanation. The Commission shall assess that information and, where appropriate, amend the implementing act laying down the common specification in question.

Article 42

Presumption of conformity with certain requirements

1. High-risk AI systems that have been trained and tested using data reflecting the specific geographical, behavioural, contextual or functional environment in which they are intended to be used shall be presumed to comply with the relevant requirements set out in Article 10(4).

2. High-risk AI systems that have a certificate or declaration of conformity under a cybersecurity scheme pursuant to Regulation (EU) 2019/881, the references of which are published in theOfficial Journal of the European Unioncomply with the cybersecurity requirements set out in Article 15 of this Regulation to the extent that the cybersecurity certificate or declaration of conformity, or parts thereof, address those requirements.

Article 43

Conformity assessment

1. For high-risk AI systems listed in point 1 of Annex III, where, when demonstrating compliance with the requirements set out in Section 2 by a high-risk AI system, the supplier has applied the harmonised standards referred to in Article 40 or, where applicable, the common specifications referred to in Article 41, the supplier shall opt for one of the following conformity assessment procedures:

a) the one based on internal control, mentioned in Annex VI, or

(b) based on the evaluation of the quality management system and the evaluation of the technical documentation, with the participation of a notified body, mentioned in Annex VII.

When demonstrating compliance with the requirements set out in Section 2 by a high-risk AI system, the supplier shall comply with the conformity assessment procedure set out in Annex VII when:

(a) the harmonised standards referred to in Article 40 do not exist and the common specifications referred to in Article 41 are not available;

b) the supplier has not applied the harmonised standard, or has only applied part of it;

c) the common specifications referred to in point (a) exist, but the supplier has not applied them;

(d) one or more of the harmonised standards referred to in point (a) have been published with a limitation, and only in the part of the standard that is the subject of the limitation.

For the purposes of the conformity assessment procedure referred to in Annex VII, the provider may choose any of the notified bodies. However, where the high-risk AI system is intended to be put into service by law enforcement authorities, immigration authorities or asylum authorities, or by Union institutions, bodies, offices or agencies, the market surveillance authority referred to in Article 74(8) or (9), as appropriate, shall act as a notified body.

2. For high-risk AI systems referred to in Annex III, points 2 to 8, suppliers shall comply with the conformity assessment procedure based on internal control referred to in Annex VI, which does not provide for the involvement of a notified body.

3. In the case of high-risk AI systems regulated by the Union harmonisation legislative acts listed in Section A of Annex I, the provider shall comply with the relevant conformity assessment procedure required by those legislative acts. The requirements set out in Section 2 of this Chapter shall apply to such high-risk AI systems and shall form part of that assessment. In addition, points 4.3, 4.4 and 4.5 of Annex VII as well as the fifth paragraph of point 4.6 of that Annex shall apply.

For the purposes of that assessment, notified bodies that have been notified pursuant to those legislative acts shall have the power to monitor the compliance of high-risk AI systems with the requirements set out in Section 2, provided that the compliance of those notified bodies with the requirements set out in Article 31(4), (5), (10) and (11) has been assessed in the context of the notification procedure pursuant to those legislative acts.

Where a legislative act listed in Section A of Annex I allows the manufacturer of the product to dispense with a third-party conformity assessment, provided that the manufacturer has applied all harmonised standards covering all relevant requirements, the manufacturer may only use this option if he has also applied the harmonised standards or, where applicable, the common specifications referred to in Article 41 covering all the requirements set out in Section 2 of this Chapter.

4. High-risk AI systems that have already been subject to a conformity assessment procedure shall be subject to a new conformity assessment procedure in the event of a substantial modification, regardless of whether a further distribution of the modified system is planned or whether it continues to be used by the person responsible for the current deployment.

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 operation that have been predetermined by the supplier at the time of the initial conformity assessment and are included in the information contained in the technical documentation referred to in point (f) of Annex IV shall not constitute substantial modifications.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 97 to amend Annexes VI and VII by updating them in the light of technical progress.

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 97 to amend paragraphs 1 and 2 of this Article in order to subject high-risk AI systems referred to in points 2 to 8 of Annex III to the conformity assessment procedure referred to in Annex VII or parts thereof. The Commission shall adopt those delegated acts taking into account the effectiveness of the conformity assessment procedure based on internal control referred to in Annex VI in preventing or minimising risks to health, safety and the protection of fundamental rights posed by such systems and the availability of adequate capacities and resources on the part of notified bodies.

Article 44

Certificates

1. Certificates issued by notified bodies in accordance with Annex VII shall be drawn up in a language which can be easily understood by the relevant authorities of the Member State in which the notified body is established.

2. Certificates shall be valid for the period indicated on them, which shall not exceed five years for AI systems referred to in Annex I and four years for AI systems referred to in Annex III. At the request of the supplier, the validity of a certificate may be extended for further periods not exceeding five years for AI systems referred to in Annex I and four years for AI systems referred to in Annex III, on the basis of a reassessment in accordance with the applicable conformity assessment procedures. Any supplement to a certificate shall remain valid provided that the certificate it supplements is valid.

3. Where a notified body finds that an AI system no longer complies with the requirements set out in Section 2, it shall, taking into account the principle of proportionality, suspend or withdraw the certificate issued or impose restrictions on it, unless compliance with those requirements is ensured by appropriate corrective measures taken by the provider of the system within an appropriate period determined by the notified body. The notified body shall state the reasons for its decision.

There will be an appeal procedure against the decisions of notified bodies, including in relation to certificates of conformity issued.

Article 45

Information obligations of notified bodies

1. Notified bodies shall inform the notifying authority:

(a) any Union certificate of assessment of technical documentation, any supplement to such certificates and any quality management system approvals issued in accordance with the requirements set out in Annex VII;

(b) any refusal, restriction, suspension or withdrawal of a Union certificate of assessment of technical documentation or of an approval of a quality management system issued in accordance with the requirements set out in Annex VII;

c) any circumstance affecting the scope or conditions of notification;

(d) any requests for information on conformity assessment activities received from market surveillance authorities;

(e) upon request, of the conformity assessment activities carried out within the scope of its notification and of any other activities carried out, including cross-border activities and subcontracting.

2. Each notified body shall inform the other notified bodies:

a) of the quality management system approvals it has refused, suspended or withdrawn and, upon request, of the quality management system approvals it has issued;

(b) Union certificates of assessment of technical documentation or supplements to such certificates which it has refused, withdrawn, suspended or otherwise restricted and, upon request, any certificates or supplements thereto which it has issued.

3. Each notified body shall provide other notified bodies carrying out similar conformity assessment activities relating to the same types of AI systems with relevant information on issues related to negative and, upon request, positive results of conformity assessments.

4. Notified bodies shall maintain the confidentiality of the information obtained in accordance with Article 78.

Article 46

Exemption from the conformity assessment procedure

1. By derogation from Article 43 and upon a duly reasoned request, any market surveillance authority may authorise the placing on the market or putting into service of specific high-risk AI systems in the territory of the Member State concerned on exceptional grounds of public security or in order to protect human life and health, the environment or critical industrial and infrastructure assets. Such authorisation shall be granted for a limited period, while the necessary conformity assessment procedures are being carried out, taking into account the exceptional grounds justifying the derogation. The procedures concerned shall be concluded without undue delay.

2. In a duly justified emergency situation on exceptional grounds of public security or in the event of a specific, significant and imminent threat to the life or physical safety of natural persons, law enforcement authorities or civil protection authorities may put into service a specific high-risk AI system without the authorisation referred to in paragraph 1, provided that such authorisation is requested during or after the use without undue delay. If the authorisation referred to in paragraph 1 is refused, the use of the high-risk AI system shall be suspended with immediate effect and all results and output information produced by such use shall be immediately discarded.

3. The authorisation referred to in paragraph 1 shall only be issued if the market surveillance authority concludes that the high-risk AI system complies with the requirements set out in Section 2. The market surveillance authority shall inform the Commission and the other Member States of any authorisation issued in accordance with paragraphs 1 and 2. This obligation shall not cover sensitive operational data relating to the activities of enforcement authorities.

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

5. If, within 15 calendar days of receipt of the notification referred to in paragraph 3, a Member State raises objections to an authorisation issued by a market surveillance authority of another Member State, or if the Commission considers that the authorisation infringes Union law or that the conclusion of the Member States concerning compliance with the system referred to in paragraph 3 is unfounded, the Commission shall consult with the relevant Member State without delay. The operators concerned shall be consulted and given the opportunity to present their views. In the light of the above, the Commission shall decide whether or not the authorisation is justified. The Commission shall forward its decision to the Member State concerned and to the relevant operators.

6. If the Commission considers that the authorisation is not justified, the market surveillance authority of the Member State concerned shall withdraw it.

7. For high-risk AI systems associated with products regulated by the Union harmonisation legislative acts listed in Section A of Annex I, only the exemptions from conformity assessment provided for in those Union harmonisation legislative acts shall apply.

Article 47

EU Declaration of Conformity

1. The supplier shall draw up an EU declaration of conformity in writing in a machine-readable format, with an electronic or handwritten signature, for each high-risk AI system and shall keep it at the disposal of the national competent authorities for a period of 10 years from the time the high-risk AI system is placed on the market or put into service. The EU declaration of conformity shall specify the high-risk AI system for which it has been drawn up. A copy of the EU declaration of conformity shall be provided to the relevant national competent authorities upon request.

2. The EU declaration of conformity shall state that the high-risk AI system concerned complies with the requirements set out in Section 2. The EU declaration of conformity shall contain the information set out in Annex V and shall be translated into a language that can be easily understood by the competent national authorities of the Member State(s) in which the high-risk AI system is placed on the market or made available on the market.

3. Where high-risk AI systems are subject to other Union harmonisation legislation which also requires an EU declaration of conformity, a single EU declaration of conformity shall be drawn up with respect to all Union law applicable to the high-risk AI system. The declaration shall contain all information necessary to determine the Union harmonisation legislation to which the declaration relates.

4. When drawing up the EU declaration of conformity, the supplier shall assume responsibility for compliance with the requirements set out in Section 2. The supplier shall keep the EU declaration of conformity up to date as appropriate.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 97 to amend Annex V by updating the content of the EU declaration of conformity set out in that Annex, in order to introduce elements which are necessary in the light of technical progress.

Article 48

CE marking

1. The CE marking shall be subject to the general principles laid down in Article 30 of Regulation (EC) No 101/2009. n.$_{\text{either}}$765/2008.

2. For high-risk AI systems that are provided digitally, a digital CE marking shall be used only if it is easily accessible through the interface from which the system is accessed or by means of an easily accessible machine-readable code or other electronic means.

3. The CE marking shall be affixed visibly, legibly and indelibly to high-risk AI systems. Where this is not possible or cannot be guaranteed due to the nature of the high-risk AI system, it shall be affixed to the packaging or accompanying documents, as appropriate.

4. Where applicable, the CE marking shall be followed by the identification number of the notified body responsible for the conformity assessment procedures laid down in Article 43. The identification number of the notified body shall be affixed by the notified body itself or, on its instructions, by the supplier or the authorised representative of the supplier. The identification number shall also appear on all advertising material stating that the high-risk AI system complies with the requirements for CE marking.

5. Where high-risk AI systems are subject to other provisions of Union law which also require the affixing of the CE marking, the CE marking shall indicate that the high-risk AI systems also comply with the requirements of those other provisions.

Article 49

Record

1. Before placing on the market or putting into service a high-risk AI system listed in Annex III, with the exception of high-risk AI systems listed in point 2 of Annex III, the provider or, where applicable, the authorised representative, shall register its system and itself in the EU database referred to in Article 71.

2. Before placing on the market or putting into service an AI system that the provider has concluded is not high-risk in accordance with Article 6(3), that provider or, where applicable, the authorised representative, shall themselves register that system in the EU database referred to in Article 71.

3. Before putting into service or using a high-risk AI system listed in Annex III, with the exception of high-risk AI systems referred to in point 2 of Annex III, those responsible for the deployment of high-risk AI systems that are public authorities, institutions, bodies, offices or agencies of the Union, or persons acting on their behalf, shall register, select the system and record its use in the EU database referred to in Article 71.

4. In the case of high-risk AI systems referred to in points 1, 6 and 7 of Annex III, in the areas of law enforcement, migration, asylum and border control management, the registration referred to in paragraphs 1, 2 and 3 of this Article shall be made in a secure non-public section of the EU database referred to in Article 71 and shall include only the information, as applicable, referred to in:

(a) Annex VIII, Section A, points 1 to 10, with the exception of points 6, 8 and 9;

(b) Annex VIII, Section B, points 1 to 5 and points 8 and 9;

(c) Annex VIII, Section C, points 1 to 3;

(d) Annex IX, points 1, 2, 3 and 5.

Only the Commission and the national authorities referred to in Article 74(8) shall have access to the respective restricted sections of the EU database listed in the first subparagraph of this paragraph.

5. High-risk AI systems referred to in Annex III, point 2, shall be registered at national level.

CHAPTER IV

TRANSPARENCY OBLIGATIONS OF SUPPLIERS AND THOSE RESPONSIBLE FOR THE DEPLOYMENT OF CERTAIN PRODUCTS AI SYSTEMS

Article 50

Transparency obligations for suppliers and those responsible for deploying certain AI systems

1. Providers shall ensure that AI systems intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system, except where it is obvious from the point of view of a reasonably informed, attentive and discerning natural person, taking into account the circumstances and context of use. This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate or prosecute criminal offences, subject to appropriate safeguards for the rights and freedoms of third parties, unless such systems are publicly available for the purpose of reporting a criminal offence.

2. Providers of AI systems, including general-purpose AI systems, generating synthetic audio, image, video or text content shall ensure that the output results of the AI system are marked in a machine-readable format and that it is possible to detect that they have been artificially generated or manipulated. Providers shall ensure that their technical solutions are efficient, interoperable, robust and reliable to the extent technically feasible, taking into account the particularities and limitations of the various types of content, the costs of implementation and the generally recognised state of the art as reflected in relevant technical standards. This obligation shall not apply to the extent that the AI systems perform a standard editing support function or do not substantially alter the input data provided by the deployer or its semantics, or where they are authorised by law to detect, prevent, investigate or prosecute criminal offences.

3. Those responsible for deploying an emotion recognition system or a biometric categorisation system shall inform natural persons exposed to it about the operation of the system and shall process their personal data in accordance with Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680, as applicable. This obligation shall not apply to AI systems used for biometric categorisation and emotion recognition that have been authorised by law to detect, prevent and investigate crime, subject to appropriate safeguards for the rights and freedoms of third parties and in accordance with Union law.

4. Those responsible for deploying an AI system that generates or manipulates images or audio or video content that constitutes a deep impersonation shall make public that such content or images have been artificially generated or manipulated. This obligation shall not apply where the law authorises its use to detect, prevent, investigate or prosecute crimes. Where the content forms part of a manifestly creative, satirical, artistic, fictional or similar work or programme, the transparency obligations set out in this section shall be limited to the obligation to make public the existence of such artificially generated or manipulated content in an appropriate manner that does not hinder the exhibition or enjoyment of the work.

Those responsible for deploying an AI system that generates or manipulates text that is published for the purpose of informing the public on matters of public interest shall disclose that the text has been artificially generated or manipulated. This obligation shall not apply where the use is authorised by law to detect, prevent, investigate or prosecute criminal offences, or where the AI-generated content has been subject to a human review or editorial control process and where a natural or legal person has editorial responsibility for the publication of the content.

5. The information referred to in paragraphs 1 to 4 shall be made available to the natural persons concerned in a clear and distinguishable manner at the latest on the occasion of their first interaction or exposure. The information shall comply with applicable accessibility requirements.

6. Paragraphs 1 to 4 shall not affect the requirements and obligations set out in Chapter III and shall be without prejudice to other transparency obligations under Union or national law for controllers deploying AI systems.

7. The AI Office shall encourage and facilitate the development of Union-wide codes of good practice to promote the effective implementation of the obligations relating to the detection and labelling of artificially generated or manipulated content. The Commission may adopt implementing acts in order to approve those codes of good practice, in accordance with the procedure laid down in Article 56(6). If it considers that the code is not adequate, the Commission may adopt an implementing act specifying common standards for the fulfilment of those obligations in accordance with the examination procedure laid down in Article 98(2).

CHAPTER V

GENERAL PURPOSE AI MODELS

SECTION 1

Classification rules

Article 51

Rules for classifying general-purpose AI models as general-purpose AI models with risk systemic

1. A general-purpose AI model shall be classified as a general-purpose AI model with systemic risk if it meets any of the following conditions:

a) has high-impact capabilities assessed using appropriate technical tools and methodologies, such as indicators and benchmarks;

(b) pursuant to a Commission decision, taken on its own initiative or following a qualified alert from the group of scientific experts, has capabilities or an impact equivalent to those set out in point (a), taking into account the criteria set out in Annex XIII.

2. A general-purpose AI model shall be presumed to have high-impact capabilities pursuant to point (a) of paragraph 1 where the cumulative amount of computation used to train it, measured in floating-point operations, is greater than 10_{25}.

3. The Commission shall adopt delegated acts in accordance with Article 97 to amend the thresholds referred to in paragraphs 1 and 2 of this Article and to supplement the benchmarks and indicators on the basis of technological developments, such as algorithmic improvements or increased hardware efficiency, where necessary to ensure that the thresholds reflect the current state of the art.

Article 52

Procedure

1. Where a general-purpose AI model fulfils the condition referred to in point (a) of Article 51(1), the relevant provider shall notify the Commission without delay and in any event within two weeks of that requirement being fulfilled or of it being known that it will be fulfilled. That notification shall include the information necessary to demonstrate that the relevant requirement is fulfilled. Where the Commission is aware of a general-purpose AI model that presents systemic risks and that has not been notified, it may decide to designate it as a model with systemic risk.

2. The provider of a general-purpose AI model that meets the condition referred to in point (a) of Article 51(1) may submit, together with its notification, sufficiently substantiated arguments demonstrating that, exceptionally, although the general-purpose AI model meets that requirement, it does not, due to its specific characteristics, present systemic risks and should therefore not be classified as a general-purpose AI model with systemic risk.

3. Where the Commission concludes that the arguments submitted pursuant to paragraph 2 are not sufficiently substantiated and that the relevant provider has not been able to demonstrate that the general-purpose AI model does not, due to its specific characteristics, present systemic risks, it shall reject those arguments and the general-purpose AI model shall be considered a general-purpose AI model with systemic risk.

4. The Commission may determine that a general-purpose AI model presents systemic risks, either ex officio or following a qualified alert from the scientific expert group pursuant to point (a) of Article 90(1), based on the criteria set out in Annex XIII.

The Commission shall be empowered to adopt delegated acts in accordance with Article 97 to amend Annex XIII by specifying and updating the criteria set out in that Annex.

5. Upon a reasoned request from a provider whose model has been designated as a general-purpose AI model with systemic risk pursuant to paragraph 4, the Commission shall take into account the request and may decide to reassess whether the general-purpose AI model can continue to be considered as posing systemic risks in accordance with the criteria set out in Annex XIII. That request shall contain objective, detailed and new reasons that have emerged since the designation decision. Providers may not request reassessment before six months have elapsed from the designation decision. If, following the reassessment, the Commission decides to maintain the designation as a general-purpose AI model with systemic risk, providers may not request another reassessment until six months have elapsed from that decision.

6. The Commission shall ensure that a list of general-purpose AI models with systemic risk is published and kept up to date, without prejudice to the need to respect and protect intellectual property rights and confidential business information or trade secrets in accordance with Union and national law.

SECTION 2

Obligations of general-purpose AI model providers

Article 53

Obligations of general-purpose AI model providers

1. General-purpose AI model providers:

(a) develop and maintain up-to-date technical documentation for the model, including information relating to the training and testing process and the results of its evaluation, which shall contain, as a minimum, the information set out in Annex XI in order to provide it, upon request, to the IA Office and to the competent national authorities;

(b) develop and maintain up-to-date information and documentation and make it available to AI system providers intending to integrate the general-purpose AI model into their AI systems. Without prejudice to the need to observe and protect intellectual property rights and confidential business information or trade secrets in accordance with Union and national law, such information and documentation shall:

(i) enable AI system providers to have a good understanding of the capabilities and limitations of the general-purpose AI model and to fulfil their obligations under this Regulation, and

(ii) contain, as a minimum, the elements set out in Annex XII;

(c) establish guidelines for compliance with Union law on copyright and related rights, and in particular for detecting and complying with, for example through cutting-edge technologies, a reservation of rights expressed in accordance with Article 4(3) of Directive (EU) 2019/790;

(d) develop and make publicly available a sufficiently detailed summary of the content used for training the general-purpose AI model, in accordance with the model provided by the AI Office.

2. The obligations set out in paragraph 1(a) and (b) shall not apply to providers of AI models that are disclosed under a free and open source licence that allows access, use, modification and distribution of the model and whose parameters, including weights, information on the architecture of the model and information on the use of the model, are made publicly available. This exception shall not apply to general-purpose AI models with systemic risk.

3. Providers of general-purpose AI models shall cooperate with the Commission and the competent national authorities, as necessary, in the exercise of their powers and authorities under this Regulation.

4. Providers of general-purpose AI models may rely on codes of practice within the meaning of Article 56 to demonstrate compliance with the obligations set out in paragraph 1 of this Article, until a harmonised standard is published. Compliance with European harmonised standards grants providers a presumption of conformity to the extent that those standards regulate those obligations. Providers of general-purpose AI models that do not adhere to an approved code of practice or do not comply with a European harmonised standard shall demonstrate compliance with their obligations by alternative means appropriate for assessment by the Commission.

5. In order to facilitate compliance with the provisions of Annex XI, in particular points 2(d) and (e) thereof, the Commission shall be empowered to adopt delegated acts in accordance with Article 97 to detail the measurement and calculation methodologies with a view to making documentation comparable and verifiable.

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 97(2) to amend Annexes XI and XII in the light of technological developments.

7. Any information or documentation obtained under this Article, including trade secrets, shall be treated in accordance with the confidentiality obligations set out in Article 78.

Article 54

Authorized representatives of general-purpose AI model providers

1. Before placing a general-purpose AI model on the Union market, providers established in third countries shall appoint, by means of a written mandate, an authorised representative who is established in the Union.

2. Suppliers shall allow their authorized representative to carry out the tasks specified in the mandate received from the supplier.

3. Authorised representatives shall carry out the tasks specified in the mandate received from the provider. They shall provide the IA Office, upon request, with a copy of the mandate in one of the official languages of the Union institutions. For the purposes of this Regulation, the mandate shall enable the authorised representative to carry out the following tasks:

(a) verify that the technical documentation indicated in Annex XI has been drawn up and that the supplier complies with all the obligations referred to in Article 53 and, where applicable, Article 55;

(b) keep a copy of the technical documentation set out in Annex XI at the disposal of the AI Office and the competent national authorities for a period of ten years from the placing on the market of the general-purpose AI model, and the contact details of the supplier who has appointed the authorised representative;

(c) provide the IA Office, upon reasoned request, with all information and documentation, including the information and documentation referred to in point (b), that are necessary to demonstrate compliance with the obligations set out in this Chapter;

(d) cooperate with the AI Office and the competent authorities, upon reasoned request, in any action they take in relation to the general-purpose AI model, including where the model is integrated into an AI system placed on the market or put into service in the Union.

4. The mandate shall enable the authorised representative to be contacted by the IA Office or the competent authorities, in addition to or instead of the provider, with reference to all matters relating to ensuring compliance with this Regulation.

5. The authorised representative shall terminate the mandate if it considers or has reason to consider that the provider is in breach of its obligations under this Regulation. In such case, it shall also immediately inform the IA Office of the termination of the mandate and the reasons therefor.

6. The obligation set out in this Article shall not apply to providers of general-purpose AI models that are disclosed under a free and open-source licence that allows access, use, modification and distribution of the model and whose parameters, including weights, information on the architecture of the model and information on the use of the model, are made publicly available, except where such general-purpose AI models present systemic risks.

SECTION 3

Obligations of providers of general-purpose AI models with systemic risk

Article 55

Obligations of providers of general-purpose AI models with systemic risk

1. In addition to the obligations listed in Articles 53 and 54, providers of general-purpose AI models with systemic risk:

a) assess the models against standardized protocols and tools that reflect the state of the art, including conducting and documenting adversarial simulation tests against the model with a view to detecting and mitigating systemic risks;

(b) assess and mitigate potential systemic risks at Union level that may arise from the development, placing on the market or use of general-purpose AI models with systemic risk, as well as the source of such risks;

(c) monitor, document and communicate, without undue delay, to the IA Office and, where appropriate, to the competent national authorities, relevant information on serious incidents and possible corrective measures to resolve them;

(d) ensure that an appropriate level of cybersecurity protection is in place for the general-purpose AI model with systemic risk and the physical infrastructure of the model.

2. Providers of general-purpose AI models with systemic risk may rely on codes of practice within the meaning of Article 56 to demonstrate compliance with the obligations set out in paragraph 1 of this Article, until a harmonised standard is published. Compliance with European harmonised standards grants providers a presumption of conformity to the extent that those standards regulate those obligations. Providers of general-purpose AI models that do not adhere to an approved code of practice or do not comply with a European harmonised standard shall demonstrate compliance with their obligations by alternative means appropriate for assessment by the Commission.

3. Any information or documentation obtained under this Article, including trade secrets, shall be treated in accordance with the confidentiality obligations set out in Article 78.

SECTION 4

Codes of good practice

Article 56

Codes of good practice

1. The AI Office shall encourage and facilitate the development of Union-wide codes of good practice in order to contribute to the proper application of this Regulation, taking into account international approaches.

2. The AI Office and the AI Council shall ensure that codes of practice cover at least the obligations set out in Articles 53 and 55, including the following issues:

(a) the means to ensure that the information referred to in Article 53(1)(a) and (b) is kept up to date with regard to market developments and technological progress;

b) the appropriate level of detail regarding the summary of the content used for the training;

(c) the determination of the type and nature of systemic risks at Union level, including their origin, where appropriate;

(d) measures, procedures and modalities for assessing and managing systemic risks at Union level, including their documentation, which shall be proportionate to the risks and take into account their severity and likelihood and the specific challenges in addressing them, taking into account how such risks may arise and materialise along the AI value chain.

3. The AI Office may invite all providers of general-purpose AI models, as well as relevant national competent authorities, to participate in the development of codes of good practice. Civil society organisations, industry, academia and other relevant stakeholders, such as downstream providers and independent experts, may contribute to the process.

4. The AI Office and the AI Council shall ensure that codes of practice clearly set out their specific objectives and contain commitments or measures, such as key performance indicators, where appropriate, to ensure the achievement of those objectives, and that they take due account of the needs and interests of all stakeholders, including affected persons, at Union level.

5. The AI Office shall ensure that participants to the codes of good practice regularly report to the AI Office on the implementation of the commitments and the actions taken and their results, including their assessment against key performance indicators, where appropriate. Key performance indicators and reporting commitments shall reflect differences in size and capacity among participants.

6. The AI Office and the AI Board shall regularly monitor and evaluate the achievement of the objectives of the codes of practice by the participants and their contribution to the proper application of this Regulation. The AI Office and the AI Board shall assess whether the codes of practice include the obligations set out in Articles 53 and 55, and shall regularly monitor and evaluate the achievement of their objectives. They shall publish their assessment of the adequacy of the codes of practice.

The Commission may, by means of an implementing act, approve a code of good practice and give it general validity within the Union. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 98(2).

7. The AI Office may invite all providers of general-purpose AI models to adhere to the codes of good practice. For providers of general-purpose AI models that do not present systemic risks, such adherence may be limited to the obligations provided for in Article 53, unless they expressly declare their interest in adhering to the full code.

8. The AI Office shall also encourage and facilitate, as appropriate, the review and adaptation of codes of good practice, in particular taking into account emerging standards. The AI Office shall assist in the assessment of available standards.

9. The codes of practice shall be finalised by 2 May 2025. The AI Office shall take the necessary measures, including inviting providers to adhere to the codes of practice in accordance with paragraph 7.

If a code of good practice has not been finalised by 2 August 2025, or if it is deemed inadequate by the AI Office following its assessment pursuant to paragraph 6 of this Article, the Commission may, by means of implementing acts, establish common rules for the fulfilment of the obligations laid down in Articles 53 and 55, covering the matters set out in paragraph 2 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

CHAPTER VI

MEASURES TO SUPPORT INNOVATION

Article 57

Controlled testing spaces for AI

1. Member States shall ensure that their competent authorities establish at least one national AI sandbox, which shall be operational by 2 August 2026. Such a sandbox may also be established jointly with the competent authorities of other Member States. The Commission may provide technical support, advice and tools for the establishment and operation of AI sandboxes.

The obligation provided for in the first subparagraph may also be fulfilled by participation in an existing controlled test area to the extent that such participation provides an equivalent level of national coverage to the participating Member States.

2. Additional AI sandboxes may also be established at regional or local level or jointly with the competent authorities of other Member States.

3. The European Data Protection Supervisor may also establish an AI sandbox for Union institutions, bodies, offices and agencies and may exercise the functions and tasks of national competent authorities pursuant to this Chapter.

4. Member States shall ensure that the competent authorities referred to in paragraphs 1 and 2 allocate sufficient resources to comply with this Article in an effective and timely manner. Where appropriate, national competent authorities shall cooperate with other relevant authorities and may allow the participation of other actors in the AI ecosystem. This Article shall not affect other controlled sandboxes established under Union or national law. Member States shall ensure an appropriate level of cooperation between the authorities overseeing those other controlled sandboxes and the national competent authorities.

5. AI sandboxes established in accordance with paragraph 1 shall provide a controlled environment that fosters innovation and facilitates the development, training, testing and validation of innovative AI systems for a limited period prior to their introduction on the market or their commissioning, in accordance with a specific sandbox plan agreed between the suppliers or potential suppliers and the competent authority. Such sandboxes may include supervised real-life testing within them.

6. Competent authorities shall, where appropriate, provide guidance, supervision and support within the AI sandbox with a view to determining the risks, in particular to fundamental rights, health and safety, to the testing and mitigation measures and their effectiveness in relation to the obligations and requirements of this Regulation and, where applicable, other provisions of Union and national law the observance of which is monitored in the AI sandbox.

7. Competent authorities shall provide providers and potential providers participating in the AI sandbox with guidance on regulatory expectations and how to comply with the requirements and obligations set out in this Regulation.

At the request of the provider or potential provider of the AI system, the competent authority shall provide written evidence of the activities successfully carried out in the sandbox. The competent authority shall also provide an exit report detailing the activities carried out in the sandbox and the related results and learning outcomes. Providers may use this documentation to demonstrate their compliance with this Regulation through the relevant conformity assessment process or market surveillance activities. In this respect, market surveillance authorities and notified bodies shall take positive account of the exit reports provided and the written evidence provided by the national competent authority, with a view to accelerating the conformity assessment procedures to a reasonable extent.

8. Subject to the confidentiality provisions of Article 78 and with the agreement of the provider or potential provider, the Commission and the AI Board shall be authorised to access the exit reports and shall take them into account, as appropriate, in the exercise of their tasks under this Regulation. If both the provider or potential provider and the competent national authority expressly agree to this, the exit report may be made public through the single information platform referred to in this Article.

9. The establishment of AI sandboxes will aim to contribute to the following objectives:

(a) improve legal certainty for compliance with this Regulation or, where applicable, other provisions of applicable Union and national law;

b) support the exchange of best practices through cooperation with authorities involved in the controlled AI sandbox;

c) foster innovation and competitiveness and facilitate the development of an AI ecosystem;

d) contribute to normative learning based on proven evidence;

(e) facilitate and accelerate access to the Union market for AI systems, in particular when provided by SMEs, including start-ups.

10. National competent authorities shall ensure that, to the extent that innovative AI systems involve the processing of personal data or fall within the scope of supervision of other national authorities or competent authorities providing or supporting access to data, national data protection authorities and other national or competent authorities are linked to the operation of the AI sandbox and involved in the supervision of such aspects to the extent permitted by their respective roles and powers.

11. AI sandboxes shall not affect the supervisory or corrective powers of competent authorities supervising the AI sandboxes, including at regional or local level. Any significant risk to health, safety and fundamental rights identified during the development and testing process of such AI systems shall lead to an appropriate reduction. National competent authorities shall be empowered to temporarily or permanently suspend the testing process, or participation in the AI sandbox if an effective reduction is not possible, and shall inform the AI Office of such decision. With the aim of supporting AI innovation in the Union, national competent authorities shall exercise their supervisory powers within the limits of the relevant law and shall use their discretion when applying legal provisions in relation to a specific AI sandbox project.

12. Suppliers and potential suppliers participating in the AI sandbox shall be liable, in accordance with Union and national law on liability, for any damage inflicted on third parties as a result of experimentation carried out in the sandbox. However, provided that potential suppliers respect the specific plan and conditions of their participation and follow in good faith the guidance provided by the competent national authority, the authorities shall not impose administrative fines for infringements of this Regulation. Where other competent authorities responsible for other provisions of Union and national law have been actively involved in the oversight of the AI system in the sandbox and have provided guidance for compliance, no administrative fines shall be imposed in relation to those provisions.

13. AI sandboxes shall be designed and implemented in such a way as to facilitate, where appropriate, cross-border cooperation between competent national authorities.

14. The competent national authorities shall coordinate their activities and cooperate within the framework of the AI Council.

15. National competent authorities shall inform the AI Office and the AI Council of the establishment of a sandbox and may seek their support and guidance. The AI Office shall make publicly available a list of planned and existing sandboxes and keep it updated in order to encourage further interaction in AI sandboxes as well as cross-border cooperation.

16. National competent authorities shall submit annual reports to the AI Office and the AI Council, for the first time one year after the establishment of the AI sandbox and thereafter every year until its completion, as well as a final report. Those reports shall provide information on the progress and results of the implementation of those sandboxes, including best practices, incidents, lessons learned and recommendations on their set-up and, where appropriate, on the application and possible revision of this Regulation, including its delegated and implementing acts, and on the application of other provisions of Union law, as monitored by the competent authorities within the framework of the sandbox. National competent authorities shall make those annual reports, or summaries thereof, publicly available online. The Commission shall, where appropriate, take into account the annual reports in the exercise of its tasks under this Regulation.

17. The Commission shall develop a single, dedicated interface containing all relevant information related to AI sandboxes to enable stakeholders to interact with AI sandboxes and raise queries with competent authorities, as well as to request non-binding guidance on the compliance of innovative products, services and business models incorporating AI technologies, in accordance with point (c) of Article 62(1). The Commission shall proactively coordinate with national competent authorities, where appropriate.

Article 58

Detailed provisions regarding controlled AI test spaces and the operation of such spaces spaces

1. In order to avoid fragmentation within the Union, the Commission shall adopt implementing acts specifying detailed arrangements for the establishment, development, implementation, operation and monitoring of AI sandboxes. The implementing acts shall include common principles on the following issues:

a) the eligibility and selection criteria for participation in the AI testbed;

b) the procedures for requesting, participating in, monitoring, exiting and terminating the AI sandbox, including the sandbox plan and exit report;

c) the conditions applicable to participants.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

2. The implementing acts referred to in paragraph 1 shall ensure:

(a) that AI sandboxes are open to any supplier or potential supplier of an AI system that submits an application and meets the eligibility and selection criteria, which shall be transparent and fair, and that the competent national authorities inform applicants of their decision within three months of the submission of the application;

(b) that AI sandboxes allow for broad and equal access and are tailored to the demand for participation; suppliers and potential suppliers will also be able to apply in partnership with deployers and other relevant third parties;

(c) the detailed provisions and conditions relating to AI sandboxes should, to the extent possible, allow national competent authorities flexibility in establishing and managing their AI sandboxes;

(d) that access to controlled AI sandboxes should be free of charge for SMEs, including start-ups, without prejudice to exceptional costs that may be recovered by the competent national authorities in a fair and proportionate manner;

(e) that suppliers and potential suppliers are facilitated, through the learning outcomes of AI sandboxes, in compliance with the conformity assessment obligations under this Regulation and the voluntary application of the codes of conduct referred to in Article 95;

(f) that AI sandboxes facilitate the participation of other relevant actors in the AI ecosystem, such as notified bodies and standardisation bodies, SMEs, including start-ups, companies, innovators, testing and experimentation facilities, research and experimentation laboratories and European digital innovation centres, centres of excellence and researchers, in order to enable and facilitate cooperation with the public and private sectors;

(g) the procedures, processes and administrative requirements for application, selection, participation in and exit from the AI sandbox are simple, easily intelligible and clearly communicated, in order to facilitate the participation of SMEs, including start-ups, with limited legal and administrative capacities, and are streamlined across the Union in order to avoid fragmentation and that participation in an AI sandbox established by a Member State or by the European Data Protection Supervisor is mutually and uniformly recognised and has the same legal effects throughout the Union;

(h) that participation in the AI sandbox is limited to a period appropriate to the complexity and scale of the project, and may be extended by the competent national authority;

(i) that AI sandboxes facilitate the development of tools and infrastructure for testing, benchmarking, evaluating and explaining the dimensions of AI systems relevant to normative learning, such as accuracy, robustness and cybersecurity, as well as measures to mitigate risks to fundamental rights and society as a whole.

3. Pre-deployment services, such as guidance on the application of this Regulation, other value-added services, such as assistance with standardisation documents and certification, and access to testing and experimentation facilities, European Digital Innovation Hubs and centres of excellence, shall be offered to potential providers participating in AI sandboxes, in particular SMEs and start-ups, where appropriate.

4. Where competent national authorities consider authorising supervised real-life testing within a controlled AI sandbox to be established pursuant to this Article, they shall specifically agree on the conditions for such testing, and in particular on appropriate safeguards, with participants, with a view to protecting fundamental rights, health and safety. Where appropriate, they shall cooperate with other competent national authorities in order to ensure consistency of practices across the Union.

Article 59

Further processing of personal data for the development of certain AI systems in the interest of the public public in the controlled testing space for AI

1. In the Sandbox, personal data lawfully collected for other purposes may be processed solely for the purposes of developing, training and testing certain AI systems in the Sandbox where all of the following conditions are met:

(a) AI systems are developed for the purposes of a public authority or other natural or legal person to protect an essential public interest in one or more of the following areas:

(i) public health and safety, including the detection, diagnosis, prevention, control and treatment of diseases and the improvement of health systems,

(ii) a high level of protection and improvement of environmental quality, protection of biodiversity, protection against pollution, ecological transition measures, climate change mitigation and adaptation measures,

iii) energy sustainability,

(iv) the security and resilience of transport systems and mobility, critical infrastructure and networks,

v) the efficiency and quality of public administration and public services;

(b) the data processed are necessary to fulfil one or more of the requirements referred to in Chapter III, Section 2, where those requirements cannot be effectively met by the processing of anonymised or synthetic data or other non-personal data;

(c) there are effective monitoring mechanisms in place to detect whether high risks to the rights and freedoms of data subjects, as referred to in Article 35 of Regulation (EU) 2016/679 and Article 39 of Regulation (EU) 2018/1725, may arise during experimentation in the controlled sandbox, as well as response mechanisms to mitigate such risks without delay and, where appropriate, stop the processing;

(d) that personal data processed in the context of the sandbox are located in a functionally separate, isolated and protected data processing environment under the control of the potential provider and that only authorised persons have access to such data;

(e) that providers may only share data originally collected in accordance with Union data protection law; personal data created in the sandbox may not leave the sandbox;

(f) the processing of personal data in the context of the sandbox does not give rise to measures or decisions affecting data subjects or affecting the implementation of their rights under Union law on the protection of personal data;

(g) that personal data processed in the context of the sandbox are protected by appropriate technical and organisational measures and are deleted after the end of participation in the sandbox or when the personal data reach the end of their retention period;

(h) log files of the processing of personal data in the context of the sandbox are retained for the duration of participation in the sandbox, unless otherwise provided for by Union or national law;

(i) a complete and detailed description of the process and logic underlying the training, testing and validation of the AI system together with the results of the testing process is maintained as part of the technical documentation referred to in Annex IV;

(j) a brief summary of the AI project developed in the sandbox, together with its objectives and expected results, is published on the website of the competent authorities; this obligation shall not cover sensitive operational data relating to the activities of law enforcement authorities, border control authorities, immigration authorities or asylum authorities.

2. Where carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security, and under the control and responsibility of law enforcement authorities, the processing of personal data in controlled AI sandboxes shall be based on specific Union or national law and shall comply with the cumulative conditions set out in paragraph 1.

3. Paragraph 1 is without prejudice to Union or national law which prohibits the processing of personal data for purposes other than those expressly mentioned in those acts, and without prejudice to Union or national law which lays down the basis for the processing of personal data necessary for developing, testing or training innovative AI systems or any other legal basis in accordance with Union law on the protection of personal data.

Article 60

Testing high-risk AI systems in real-world conditions outside of controlled test spaces for AI

1. Suppliers or potential suppliers of high-risk AI systems listed in Annex III may carry out real-world testing of high-risk AI systems outside the controlled AI sandboxes in accordance with this Article and with the real-world test plan referred to in this Article, without prejudice to the prohibitions set out in Article 5.

The Commission shall adopt, by means of an implementing act, the detailed elements of the real-life test plan. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

This paragraph is without prejudice to Union or national law on real-life testing of high-risk AI systems associated with products covered by the Union harmonisation legislative acts listed in Annex I.

2. Suppliers or potential suppliers may carry out testing of high-risk AI systems referred to in Annex III under real-life conditions at any time prior to the placing on the market or putting into service of the AI system on their own behalf or in partnership with one or more deployers or potential deployers.

3. Testing of high-risk AI systems under real-world conditions pursuant to this Article shall be without prejudice to any ethical review required by Union or national law.

4. Suppliers or potential suppliers may carry out tests under real conditions only when all of the following conditions are met:

(a) the supplier or potential supplier has drawn up a real-world test plan and submitted it to the market surveillance authority of the Member State in which the real-world tests are to be carried out;

(b) the market surveillance authority of the Member State in which the real-life tests are to be carried out has approved the real-life tests and the real-life test plan; if the market surveillance authority does not reply within 30 days, the real-life tests and the real-life test plan shall be deemed to have been approved; where national law does not provide for tacit approval, the real-life tests shall be subject to authorisation in this case as well;

(c) the supplier or potential supplier, with the exception of suppliers or potential suppliers of high-risk AI systems referred to in points 1, 6 and 7 of Annex III in the areas of enforcement, migration, asylum and border control management and of high-risk AI systems referred to in point 2 of Annex III, has registered the real-life testing in accordance with Article 71(4) with a unique Union-wide identification number and the information set out in Annex IX; the supplier or potential supplier of high-risk AI systems referred to in points 1, 6 and 7 of Annex III in the areas of enforcement, migration, asylum and border control management has registered the real-life testing in the non-public part of the EU database in accordance with point (d) of Article 49(4) with a unique Union-wide identification number and the information set out therein; the supplier or potential supplier of high-risk AI systems referred to in point 2 of Annex III has registered real-life testing in accordance with Article 49(5);

(d) the supplier or potential supplier carrying out the tests under real conditions is established in the Union or has appointed a legal representative who is established in the Union;

(e) data collected and processed for the purposes of real-life testing shall only be transferred to third countries if appropriate and applicable safeguards are in place under Union law;

(f) the tests under real conditions do not last longer than necessary to achieve their objectives and, in any case, not more than six months, which may be extended for a further period of six months, subject to prior notification by the supplier or potential supplier to the market surveillance authority, accompanied by an explanation of the need for such an extension;

g) real-life test subjects who are members of vulnerable groups due to their age or disability have adequate protection;

(h) where a supplier or potential supplier organises real-world testing in cooperation with one or more deployers or potential deployers, the latter shall have been informed of all aspects of the testing relevant to their decision to participate and shall have received relevant instructions on the use of the AI system referred to in Article 13; the supplier or potential supplier and the deployer or potential deployer shall reach an agreement detailing their roles and responsibilities with a view to ensuring compliance with the provisions relating to real-world testing under this Regulation and other provisions of applicable Union and national law;

(i) the subjects of real-world testing have given informed consent in accordance with Article 61 or, in the area of enforcement where attempting to obtain informed consent would prevent the AI system from being tested, the testing itself and the results of the real-world testing will have no negative impact on the subjects, whose personal data will be erased after the test has been carried out;

(j) real-world testing is effectively supervised by the supplier or potential supplier and by the deployers or potential deployers using persons appropriately qualified in the relevant field and with the necessary skills, training and authority to perform their tasks;

k) the AI system's predictions, recommendations or decisions can be effectively reversed and discarded.

5. Any subject of real-life testing or his or her legally designated representative, as appropriate, may, without suffering any disadvantage and without having to provide any justification, withdraw from the testing at any time by withdrawing his or her informed consent and requesting the immediate and permanent deletion of his or her personal data. The withdrawal of informed consent will not affect activities already completed.

6. In accordance with Article 75, Member States shall confer on their market surveillance authorities the power to require suppliers and potential suppliers to provide information, to carry out unannounced remote inspections or toin situand to monitor the conduct of real-world testing and related high-risk AI systems. Market surveillance authorities shall use such powers to ensure that real-world testing is conducted safely.

7. Any serious incident detected during the course of real-world testing shall be reported to the national market surveillance authority in accordance with Article 73. The supplier or potential supplier shall take immediate mitigation measures or, failing that, suspend real-world testing until such mitigation has taken place or terminate the testing. The supplier or potential supplier shall establish a procedure for the rapid recovery of the AI system in the event that real-world testing is terminated.

8. The supplier or potential supplier shall notify the national market surveillance authority of the Member State in which the real-world testing is to be carried out of the suspension or termination of the real-world testing and the final results.

9. The supplier or potential supplier shall be liable, in accordance with applicable Union and national liability law, for any damage caused in the course of its tests under real conditions.

Article 61

Informed consent to participate in tests under real conditions outside the controlled spaces of Testing for AI

1. For the purposes of real-life testing pursuant to Article 60, freely given informed consent shall be obtained from test subjects prior to participation in such testing and after having been provided with concise, clear, relevant and comprehensible information regarding:

a) the nature and objectives of the tests under real conditions and the possible inconveniences associated with their participation;

b) the conditions under which the real-world testing will be conducted, including the expected duration of the subject(s)' participation;

(c) their rights and guarantees relating to their participation, in particular their right to refuse to participate and the right to withdraw from the real-life tests at any time without suffering any disadvantage and without having to provide any justification;

(d) provisions for requesting reversal or discarding of predictions, recommendations or decisions of the AI system;

(e) the unique Union-wide identification number of the real-life test in accordance with point (c) of Article 60(4) and the contact details of the supplier or its legal representative from whom further information may be obtained.

2. Informed consent will be dated and documented, and a copy will be given to the test subjects or their legal representatives.

Article 62

Measures targeting suppliers and those responsible for deployment, in particular SMEs, including companies emerging

1. Member States shall take the following measures:

(a) provide SMEs, including start-ups, having a registered office or a branch in the Union with priority access to the AI sandboxes, provided that they fulfil the eligibility conditions and selection criteria; priority access shall not prevent other SMEs, including start-ups, other than those referred to in this paragraph from accessing the AI sandbox, provided that they also fulfil the eligibility conditions and selection criteria;

(b) organise targeted awareness-raising and training activities on the application of this Regulation tailored to the needs of SMEs, including start-ups, deployers and, where appropriate, local public authorities;

(c) use existing and, where appropriate, establish new dedicated channels for communication with SMEs, including start-ups, deployers and other innovative actors, as well as, where appropriate, local public authorities, in order to provide advice and answer questions raised regarding the application of this Regulation, including in relation to participation in AI sandboxes;

d) encourage the participation of SMEs and other relevant stakeholders in the standardization development process.

2. The specific interests and needs of SME suppliers, including start-ups, shall be taken into account when setting fees for conformity assessment under Article 43, and such fees shall be reduced in proportion to their size, the size of the market and other relevant indicators.

3. The IA Office shall take the following measures:

(a) provide standardised templates for the areas covered by this Regulation, as specified by the AI Council in its request;

(b) develop and maintain a single information platform providing user-friendly information in relation to this Regulation for all operators in the Union;

(c) organise appropriate communication campaigns to raise awareness of the obligations arising from this Regulation;

d) assess and promote convergence of best practices in public procurement procedures in relation to AI systems.

Article 63

Exceptions for specific operators

1. Micro-enterprises within the meaning of Recommendation 2003/361/EC may comply with certain elements of the quality management system required by Article 17 of this Regulation in a simplified manner, provided that they do not have associated undertakings or linked undertakings within the meaning of that Recommendation. To this end, the Commission shall draw up guidelines on the elements of the quality management system that can be complied with in a simplified manner taking into account the needs of micro-enterprises without affecting the level of protection or the need to comply with the requirements relating to high-risk AI systems.

2. Paragraph 1 of this Article shall not be construed as exempting such operators from compliance with any other requirements or obligations set out in this Regulation, including those set out in Articles 9, 10, 11, 12, 13, 14, 15, 72 and 73.

CHAPTER VII

GOVERNANCE

SECTION 1

Governance at Union level

Article 64

AI Office

1. The Commission shall develop the Union's expertise and capabilities in the field of AI through the AI Office.

2. Member States shall facilitate the tasks entrusted to the AI Office, as reflected in this Regulation.

Article 65

Creation and structure of the European Artificial Intelligence Council

1. A European Artificial Intelligence Council (hereinafter referred to as the ‘AI Council’) is hereby established.

2. The AI Board shall be composed of one representative per Member State. The European Data Protection Supervisor shall participate as an observer. The AI Office shall also attend the meetings of the AI Board without voting. The AI Board may invite other Union and national authorities, bodies or experts to the meetings on a situation-by-case basis, where the topics discussed are relevant to them.

3. Each representative shall be appointed by his or her Member State for a period of three years, renewable once.

4. Member States shall ensure that their representatives on the AI Council:

(a) have the relevant powers and competences in their Member State to be able to actively contribute to the fulfilment of the tasks of the IA Board referred to in Article 66;

(b) be designated as a single point of contact for the AI Council and, where appropriate, taking into account the needs of Member States, as a single point of contact for stakeholders;

(c) be empowered to facilitate coherence and coordination between the competent national authorities in their Member State in relation to the application of this Regulation, including by collecting relevant data and information to fulfil their duties within the IA Council.

5. The designated representatives of the Member States shall adopt the Rules of Procedure of the IA Board by a two-thirds majority. The Rules of Procedure shall set out, in particular, the procedures for the selection process, the term of office and the specifications of the functions of the Chair, the detailed voting modalities and the organisation of the activities of the IA Board and its subgroups.

6. The IA Board shall establish two permanent subgroups in order to provide a platform for cooperation and exchange between market surveillance authorities and to notify authorities on issues related to market surveillance and notified bodies, respectively.

The permanent market surveillance subgroup should act as an administrative cooperation group (ADCO) for this Regulation within the meaning of Article 30 of Regulation (EU) 2019/1020.

The IA Council may establish other subgroups of a permanent or temporary nature, as appropriate, to examine specific matters. Where appropriate, representatives of the consultative forum referred to in Article 67 may be invited to such subgroups or to specific meetings of such subgroups as observers.

7. The AI Council shall be organized and managed in such a way as to preserve the objectivity and impartiality of its activities.

8. The AI Board shall be chaired by one of the representatives of the Member States. The AI Office shall act as the secretariat of the AI Board, convene meetings at the request of the Chair and draw up the agenda in accordance with the tasks of the AI Board under this Regulation and its Rules of Procedure.

Article 66

AI Council Functions

The AI Council shall provide advice and assistance to the Commission and the Member States to facilitate the consistent and effective application of this Regulation. To this end, the AI Council may, in particular:

(a) contribute to coordination between the competent national authorities responsible for the application of this Regulation and, in cooperation with and subject to agreement between the market surveillance authorities concerned, support the joint activities of market surveillance authorities referred to in Article 74(11);

b) collect and share technical and regulatory knowledge and best practices among Member States;

(c) provide advice on the application of this Regulation, in particular as regards compliance with the rules on general-purpose AI models;

(d) contribute to the harmonisation of administrative practices in the Member States, including in relation to the exemption from conformity assessment procedures referred to in Article 46, the operation of controlled sandboxes for AI and real-world testing referred to in Articles 57, 59 and 60;

(e) upon request of the Commission or on its own initiative, issue written recommendations and opinions on any relevant matter relating to the implementation of this Regulation and its consistent and effective application, for example:

(i) on the development and application of codes of conduct and codes of good practice in accordance with this Regulation and the Commission guidelines,

(ii) on the evaluation and review of this Regulation pursuant to Article 112, including as regards serious incident reports referred to in Article 73, and the functioning of the EU database referred to in Article 71, the preparation of delegated or implementing acts, and as regards possible adaptations of this Regulation to the Union harmonisation legislative acts listed in Annex I,

(iii) on existing technical specifications or standards relating to the requirements set out in Chapter III, Section 2,

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

(v) on trends, such as Europe's global competitiveness in AI, the adoption of AI in the Union and the development of digital capabilities,

(vi) on trends in the changing typology of AI value chains, in particular on the resulting implications in terms of accountability,

(vii) on the possible need to amend Annex III in accordance with Article 7 and on the possible need to review Article 5 in accordance with Article 112, taking into account relevant available evidence and recent technological developments;

(f) support the Commission in promoting AI literacy, public awareness and understanding of the benefits, risks, safeguards and rights and obligations in relation to the use of AI systems;

(g) facilitate the development of common criteria and shared understanding among market operators and competent authorities of the relevant concepts provided for in this Regulation, for example by contributing to the development of benchmarks;

(h) cooperate, where appropriate, with other Union institutions, bodies, offices and agencies, as well as with relevant Union expert groups and networks, in particular in the areas of product safety, cybersecurity, competition, digital and media services, financial services, consumer protection, and the protection of data and fundamental rights;

(i) contribute to effective cooperation with the competent authorities of third countries and with international organisations;

(j) assist the competent national authorities and the Commission in developing the technical and organisational expertise necessary for the implementation of this Regulation, for example by contributing to the assessment of training needs of Member States' staff involved in its implementation;

(k) assist the AI Office in supporting national competent authorities in establishing and developing AI sandboxes, and facilitate cooperation and information exchange between AI sandboxes;

l) contribute to the development of guidance documents and provide relevant advice thereon;

(m) provide advice to the Commission on international AI matters;

(n) issue opinions to the Commission on qualified alerts concerning general-use AI models;

(o) receive opinions from Member States on qualified alerts concerning general-purpose AI models and on national experiences and practices in the supervision and enforcement of AI systems, in particular systems integrating general-purpose AI models.

Article 67

Advisory forum

1. An advisory forum shall be established to provide expertise and advice to the AI Board and the Commission, as well as to contribute to their tasks under this Regulation.

2. The composition of the consultative forum shall represent a balanced selection of stakeholders, including industry, start-ups, SMEs, civil society and academia. The composition of the consultative forum shall be balanced with regard to commercial and non-commercial interests and, within the category of commercial interests, with regard to SMEs and other enterprises.

3. The Commission shall appoint the members of the advisory forum, in accordance with the criteria set out in paragraph 2, from among interested parties with recognised expertise in the field of AI.

4. The term of office of the members of the consultative forum shall be two years and may be extended for a maximum of four years.

5. The European Union Agency for Fundamental Rights, the European Union Agency for Cybersecurity, the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications Standards Institute (ETSI) shall be permanent members of the advisory forum.

6. The consultative forum shall establish its own rules of procedure. It shall elect two co-chairs from among its members, in accordance with the criteria set out in paragraph 2. The co-chairs shall have a term of office of two years, renewable once.

7. The consultative forum shall hold meetings at least twice a year. It may invite experts and other interested parties to its meetings.

8. The advisory forum may draw up written opinions, recommendations and contributions at the request of the IA Board or the Commission.

9. The advisory forum may establish permanent or temporary subgroups, as appropriate, to examine specific issues related to the objectives of this Regulation.

10. The consultative forum shall draw up an annual report on its activities. This report shall be made available to the public.

Article 68

Group of independent scientific experts

1. The Commission shall, by means of an implementing act, adopt provisions on the establishment of a group of independent scientific experts (hereinafter referred to as the 'scientific expert group') to support the enforcement activities provided for in this Regulation. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 98(2).

2. The scientific expert group shall be composed of experts selected by the Commission on the basis of up-to-date scientific or technical knowledge in the field of AI required for the tasks set out in paragraph 3, and shall be able to demonstrate that it meets all of the following conditions:

a) specialised knowledge and particular competences, and scientific or technical knowledge in the field of AI;

b) independence from any provider of AI systems or general-purpose AI models;

c) ability to carry out activities with diligence, precision and objectivity.

The Commission, in consultation with the IA Board, shall determine the number of experts in the group in accordance with the required needs and shall ensure fair geographical and gender representation.

3. The Scientific Expert Group shall advise and support the AI Office, in particular with regard to the following functions:

(a) support the implementation and enforcement of this Regulation with regard to general-purpose AI systems and models, in particular:

(i) alerting the AI Office to potential Union-wide systemic risks from general-purpose AI models, in accordance with Article 90,

(ii) contributing to the development of tools and methodologies to assess the capabilities of general-purpose AI systems and models, including through benchmarks,

iii) advising on the classification of general-purpose AI models with systemic risk,

(iv) advising on the classification of various general-purpose AI systems and models,

v) contributing to the development of tools and models;

b) support the work of market surveillance authorities, at their request;

(c) support cross-border market surveillance activities referred to in Article 74(11), without prejudice to the powers of market surveillance authorities;

(d) support the IA Office in the exercise of its tasks in the context of the Union safeguard procedure pursuant to Article 81.

4. The experts of the group shall perform their duties impartially and objectively and shall ensure the confidentiality of information and data obtained in the performance of their duties and activities. They shall neither seek nor accept instructions from anyone in the performance of their duties under paragraph 3. Each expert shall complete a declaration of interests which shall be made public. The IA Office shall establish systems and procedures to actively manage and prevent potential conflicts of interest.

5. The implementing act referred to in paragraph 1 shall include provisions on the conditions, procedures and detailed arrangements for the scientific expert group and its members to issue alerts and to request the assistance of the AI Office in carrying out the functions of the scientific expert group.

Article 69

Access to experts by Member States

1. Member States may call upon experts from the scientific expert group to support their enforcement activities under this Regulation.

2. Member States may be required to pay fees for advice and support provided by experts. The structure and amount of the fees, as well as the scale and structure of the recoverable costs, shall be set out in the implementing act referred to in Article 68(1), taking into account the objectives of the proper implementation of this Regulation, cost-effectiveness and the need to ensure that all Member States have effective access to experts.

3. The Commission shall facilitate timely access by Member States to experts, as necessary, and shall ensure that the combination of support activities carried out by the Union AI testing support structures pursuant to Article 84 and by experts pursuant to this Article is organised in an efficient manner and offers the greatest possible added value.

SECTION 2

Competent national authorities

Article 70

Designation of competent national authorities and single points of contact

1. Each Member State shall establish or designate at least one notifying authority and at least one market surveillance authority as national competent authorities for the purposes of this Regulation. Those national competent authorities shall exercise their powers in an independent, impartial and unbiased manner, in order to preserve the objectivity of their activities and tasks and to ensure the application and enforcement of this Regulation. Members of those authorities shall refrain from any act incompatible with their tasks. Provided that those principles are respected, those activities and tasks may be carried out by one or more designated authorities, in accordance with the organisational needs of the Member State.

2. Member States shall communicate to the Commission the identity of the notifying authorities and the market surveillance authorities and the tasks of those authorities and any subsequent changes thereto. Member States shall make publicly available, by electronic means, information on how to contact the competent authorities and single contact points by 2 August 2025. Member States shall designate a market surveillance authority to act as a single contact point for this Regulation and shall notify the Commission of the identity of that point. The Commission shall make the list of single contact points publicly available.

3. Member States shall ensure that their national competent authorities have adequate technical, financial and human resources and infrastructure to effectively carry out their tasks under this Regulation. In particular, national competent authorities shall have at all times sufficient staff whose skills and expertise shall include in-depth knowledge of AI, data and data computing technologies; the protection of personal data, cybersecurity, risks to fundamental rights, health and safety, and knowledge of applicable legal rules and requirements. Member States shall assess and, where necessary, update annually the skills and resource requirements referred to in this paragraph.

4. The competent national authorities shall take appropriate measures to ensure an adequate level of cybersecurity.

5. In carrying out their duties, the competent national authorities shall act in accordance with the confidentiality obligations set out in Article 78.

6. By 2 August 2025 and every two years thereafter, Member States shall submit to the Commission a report on the state of the financial and human resources of the national competent authorities, including an assessment of their adequacy. The Commission shall forward that information to the IA Board for discussion and, where appropriate, for recommendations.

7. The Commission shall facilitate the exchange of experiences between the competent national authorities.

8. National competent authorities may provide guidance and advice on the application of this Regulation, in particular to SMEs, including start-ups, taking into account guidance and advice from the AI Council and the Commission, as appropriate. Whenever a national competent authority intends to provide guidance and advice in relation to an AI system in areas regulated by other acts of Union law, national competent authorities shall be consulted in accordance with those acts, as appropriate.

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

CHAPTER VIII

EU DATABASE FOR HIGH-RISK AI SYSTEMS

Article 71

EU database for high-risk AI systems listed in ANNEX III

1. The Commission, in collaboration with the Member States, shall establish and maintain an EU database containing the information referred to in paragraphs 2 and 3 of this Article concerning high-risk AI systems referred to in Article 6(2) that are registered pursuant to Articles 49 and 60 and AI systems that are not considered high-risk pursuant to Article 6(3) and that are registered pursuant to Article 6(4) and Article 49. The Commission shall consult relevant experts when establishing the functional specifications of that database and the AI Council when updating it.

2. The data listed in Annex VIII, Sections A and B, shall be entered into the EU database by the supplier or, where applicable, by the authorised representative.

3. The data listed in Section C of Annex VIII shall be entered into the EU database by, or acting on behalf of, the person responsible for the deployment, which is a public authority, body, office or agency, in accordance with Article 49(3) and (4).

4. With the exception of the section referred to in Article 49(4) and Article 60(4)(c), information held in the EU database and recorded in accordance with Article 49 shall be accessible and available to the public in a user-friendly manner. The information must be easy to navigate and machine-readable. Information recorded in accordance with Article 60 may only be accessed by market surveillance authorities and the Commission, unless the potential supplier or the supplier has given its consent for the information to also be made publicly accessible.

5. The EU database shall only contain personal data to the extent necessary for the collection and processing of information in accordance with this Regulation. Such information shall include the names and contact details of the natural persons responsible for the system registration and having legal authority to represent the provider or the deployer, as applicable.

6. The Commission shall be the controller of the EU database and shall provide appropriate technical and administrative support to suppliers, potential suppliers and deployers. The EU database shall comply with applicable accessibility requirements.

CHAPTER IX

POST-MARKETING SURVEILLANCE, INFORMATION EXCHANGE AND MARKET SURVEILLANCE

SECTION 1

Post-marketing surveillance

Article 72

Post-marketing surveillance by suppliers and post-marketing surveillance plan for high-risk AI systems

1. Suppliers shall establish and document a post-market surveillance system in a manner proportionate to the nature of the AI technologies and the risks of high-risk AI systems.

2. The post-market surveillance system shall actively and systematically collect, document and analyse relevant data that may be provided by deployers or collected through other sources on the operation of high-risk AI systems throughout their lifetime, and which enables the provider to assess the continued compliance of the AI systems with the requirements set out in Chapter III, Section 2. Where appropriate, post-market surveillance shall include an analysis of the interaction with other AI systems. This obligation shall not cover sensitive operational data of deployers who are enforcement authorities.

3. The post-market surveillance system shall be based on a post-market surveillance plan. The post-market surveillance plan shall be part of the technical documentation referred to in Annex IV. The Commission shall adopt an implementing act laying down detailed provisions constituting a template for the post-market surveillance plan and the list of elements to be included in it by 2 February 2026. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 98(2).

4. For high-risk AI systems regulated by the Union harmonisation legislative acts listed in Section A of Annex I, where a post-market surveillance system and plan have already been established pursuant to those acts, in order to ensure consistency, avoid duplication and minimise additional burdens, providers may choose to integrate, as appropriate, the necessary elements described in paragraphs 1, 2 and 3, using the template referred to in paragraph 3, into systems and plans already in place under that legislation, provided that it achieves an equivalent level of protection.

The first subparagraph of this paragraph shall also apply to high-risk AI systems referred to in point 5 of Annex III placed on the market or put into service by financial institutions subject to requirements relating to their governance, systems or internal processes under Union financial services law.

SECTION 2

Exchange of information on serious incidents

Article 73

Reporting serious incidents

1. Providers of high-risk AI systems placed on the Union market shall notify any serious incident to the market surveillance authorities of the Member States in which the incident occurred.

2. The notification referred to in paragraph 1 shall be made immediately after the provider has established a causal link between the AI   system and the serious incident or the reasonable likelihood that such a link exists and, in any case, no later than 15 days after the provider or, where applicable, the person responsible for the deployment, becomes aware of the serious incident.

The period for notification referred to in the first paragraph shall take into account the magnitude of the serious incident.

3. Notwithstanding paragraph 2 of this Article, in the case of a widespread infringement or a serious incident as defined in point (b) of Article 3, point 49, the notification referred to in paragraph 1 of this Article shall be made immediately and at the latest two days after the provider or, where applicable, the person responsible for the deployment becomes aware of the incident.

4. Notwithstanding paragraph 2, in the event of the death of a person, notification shall be made immediately after the provider or the deployer has established — or as soon as the provider or the deployer suspects — a causal link between the high-risk AI system and the serious incident, but no later than ten days from the date on which the provider or, where applicable, the deployer becomes aware of the serious incident.

5. Where necessary to ensure timely notification, the provider or, where applicable, the deployer may initially submit an incomplete notification, followed by a complete notification.

6. After notifying a serious incident pursuant to paragraph 1, the provider shall without delay carry out the necessary investigations in relation to the serious incident and the affected AI system. This shall include a risk assessment of the incident and corrective measures.

The provider shall cooperate with the competent authorities and, where applicable, the notified body concerned during the investigations referred to in the first subparagraph and shall not take any action that would modify the affected AI system in a way that could impact any subsequent assessment of the causes of the incident without first informing the competent authorities of that action.

7. Following receipt of a notification concerning a serious incident referred to in point (c) of Article 3, point 49, the relevant market surveillance authority shall inform the national public authorities or bodies referred to in Article 77(1). The Commission shall develop specific guidance to facilitate compliance with the obligations set out in paragraph 1 of this Article. That guidance shall be published by 2 August 2025 and shall be regularly assessed.

8. The market surveillance authority shall take appropriate measures as provided for in Article 19 of Regulation (EU) 2019/1020 within seven days of the date on which it receives the notification referred to in paragraph 1 of this Article and shall follow the notification procedures provided for in that Regulation.

9. In the case of high-risk AI systems referred to in Annex III placed on the market or put into service by providers which are subject to Union legislative instruments laying down reporting obligations equivalent to those laid down in this Regulation, the reporting of serious incidents shall be limited to those referred to in point (c) of Article 3, point 49.

10. In the case of high-risk AI systems that are security components of devices, or that are themselves devices, regulated by Regulation (EU) 2017/745 and (EU) 2017/746, the notification of serious incidents shall be limited to those referred to in point (c) of Article 3, point 49 of this Regulation, and shall be made to the competent national authority chosen for that purpose by the Member States in which the incident occurred.

11. The competent national authorities shall immediately inform the Commission of any serious incident, regardless of whether they have taken any action in this regard, in accordance with Article 20 of Regulation (EU) 2019/1020.

SECTION 3

Guarantee of compliance

Article 74

Market surveillance and control of AI systems on the EU market

1. Regulation (EU) 2019/1020 shall apply to AI systems regulated by this Regulation. For the purposes of ensuring effective compliance with this Regulation:

(a) any reference to an economic operator pursuant to Regulation (EU) 2019/1020 shall be deemed to include all operators referred to in Article 2(1) of this Regulation;

(b) any reference to a product under Regulation (EU) 2019/1020 shall be deemed to include all AI systems falling within the scope of this Regulation.

2. As part of their reporting obligations under Article 34(4) of Regulation (EU) 2019/1020, market surveillance authorities shall annually report to the Commission and the relevant national competition authorities on any information collected in the course of market surveillance activities that may be of potential relevance for the enforcement of Union competition law. They shall also annually report to the Commission on the use of prohibited practices that have occurred during that year and on the measures taken.

3. For high-risk AI systems associated with products regulated by the Union harmonisation legislative acts listed in Section A of Annex I, the market surveillance authority for the purposes of this Regulation shall be the authority responsible for market surveillance activities designated pursuant to those legislative acts.

By way of derogation from the first subparagraph, in appropriate circumstances, Member States may designate another relevant authority as market surveillance authority, provided that coordination is ensured with the relevant sectoral market surveillance authorities responsible for the implementation of the Union harmonisation legislative acts listed in Annex I.

4. The procedures referred to in Articles 79 to 83 of this Regulation shall not apply to AI systems associated with products regulated by the Union harmonisation legislative acts listed in Section A of Annex I where those legislative acts already provide for procedures ensuring an equivalent level of protection having the same objective. In such cases, the relevant sectoral procedures shall apply.

5. Without prejudice to the powers of market surveillance authorities under Article 14 of Regulation (EU) 2019/1020, for the purposes of ensuring the effective implementation of this Regulation, market surveillance authorities may exercise remotely the powers referred to in points (d) and (j) of Article 14(4) of that Regulation, as appropriate.

6. In the case of high-risk AI systems placed on the market, put into service or used by financial institutions regulated under Union financial services law, the market surveillance authority for the purposes of this Regulation shall be the relevant national authority responsible for the financial supervision of such institutions under that law, to the extent that the placing on the market, putting into service or use of the AI system is directly related to the provision of those financial services.

7. By way of derogation from paragraph 6, in appropriate circumstances and provided that coordination is ensured, the Member State may designate another relevant authority as market surveillance authority for the purposes of this Regulation.

National market surveillance authorities supervising credit institutions regulated by Directive 2013/36/EU and participating in the Single Supervisory Mechanism established by Regulation (EU) No.$_{\text{either}}$1024/2013 shall without delay communicate to the European Central Bank any information obtained in the course of their market surveillance activities that may be relevant to the prudential supervision tasks of the European Central Bank specified in that Regulation.

8. For high-risk AI systems listed in point 1 of Annex III to this Regulation, to the extent that the systems are used for the purposes of law enforcement, border management and justice and democracy, and for high-risk AI systems listed in points 6, 7 and 8 of Annex III to this Regulation, Member States shall designate as market surveillance authorities for the purposes of this Regulation either the competent data protection supervisory authorities pursuant to Regulation (EU) 2016/679 or Directive (EU) 2016/680 or any other authority designated under the same conditions set out in Articles 41 to 44 of Directive (EU) 2016/680. Market surveillance activities shall in no way affect the independence of judicial authorities or otherwise interfere with their activities in the exercise of their judicial function.

9. Where Union institutions, bodies, offices and agencies fall within the scope of this Regulation, the European Data Protection Supervisor shall act as their market surveillance authority, except in relation to the Court of Justice of the European Union when acting in the exercise of its judicial function.

10. Member States shall facilitate coordination between market surveillance authorities designated pursuant to this Regulation and other relevant national authorities or bodies responsible for overseeing the application of Union harmonisation legislation referred to in Annex I or other provisions of Union law that may be relevant to high-risk AI systems referred to in Annex III.

11. Market surveillance authorities and the Commission may propose joint activities, including joint investigations, to be carried out either by market surveillance authorities or by market surveillance authorities together with the Commission, with the aim of promoting compliance, identifying non-compliance, raising awareness or providing guidance in relation to this Regulation with regard to specific categories of high-risk AI systems that pose a serious risk in two or more Member States in accordance with Article 9 of Regulation (EU) 2019/1020. The AI Office shall provide coordination support to joint investigations.

12. Without prejudice to the powers provided for in Regulation (EU) 2019/1020, and where appropriate and limited to what is necessary for the performance of their tasks, providers shall grant market surveillance authorities full access to documentation as well as training, validation and testing data sets used for the development of high-risk AI systems, including, where appropriate and subject to security safeguards, through application programming interfaces (APIs) or other relevant technical tools and means allowing remote access.

13. Market surveillance authorities shall be granted access to the source code of the high-risk AI system upon reasoned request and only if the following two conditions are met:

a) access to the source code is necessary to assess the compliance of a high-risk AI system with the requirements set out in Chapter III, Section 2, and

b) all testing or audit procedures and checks based on data and documentation provided by the supplier have been exhausted or have proven insufficient.

14. Any information or documentation obtained by market surveillance authorities shall be treated in accordance with the confidentiality obligations set out in Article 78.

Article 75

Mutual assistance, market surveillance and control of general-purpose AI systems

1. Where an AI system is based on a general-purpose AI model and both the model and the system are developed by a single provider, the AI Office shall be empowered to monitor and supervise the compliance of that AI system with the obligations under this Regulation. In carrying out those monitoring and supervision tasks, the AI Office shall have all the powers of an authority provided for in this Section and in Regulation (EU) 2019/1020.

2. Where relevant market surveillance authorities have sufficient grounds to consider that general-purpose AI systems that may be directly used by deployers for at least one of the purposes classified as high-risk under this Regulation do not comply with the requirements set out in this Regulation, they shall cooperate with the AI Office to carry out compliance assessments and report thereon to the AI Board and the other market surveillance authorities.

3. Where a market surveillance authority is unable to conclude its investigation into the high-risk AI system due to the lack of access to certain information relating to the general-purpose AI model, despite having made all appropriate efforts to obtain that information, it may submit a reasoned request to the AI Office for access to that information. In such a case, the AI Office shall provide the requesting authority without delay and in any case within 30 days with all information that the AI Office considers relevant for determining whether a high-risk AI system is non-compliant. Market surveillance authorities shall keep the information obtained in accordance with Article 78 of this Regulation confidential.mutatis mutandisthe procedure provided for in Chapter VI of Regulation (EU) 2019/1020.

Article 76

Supervision of real-life testing by market surveillance authorities

1. Market surveillance authorities shall have the necessary powers and competences to ensure that real-life testing complies with this Regulation.

2. Where real-life testing of supervised AI systems is carried out within an AI sandbox pursuant to Article 58, market surveillance authorities shall verify compliance with Article 60 as part of their supervisory role in the AI sandbox. Those authorities may, as appropriate, allow the supplier or potential supplier to carry out real-life testing, as an exception to the conditions set out in points (f) and (g) of Article 60(4).

3. Where a market surveillance authority has been informed by the potential supplier, the supplier or a third party of a serious incident or has other reasons to believe that the conditions set out in Articles 60 and 61 are not met, it may take one of the following decisions in its territory, as appropriate:

a) suspend or terminate tests under real conditions;

b) require the supplier or potential supplier and the person responsible for the deployment or the person responsible for the potential deployment to modify any aspect of the real-world testing.

4. Where a market surveillance authority has taken a decision referred to in paragraph 3 of this Article or has raised an objection within the meaning of Article 60(4)(b), the decision or objection shall state the reasons for the decision and indicate the means available to the supplier or potential supplier to challenge the decision or objection.

5. Where appropriate, where a market surveillance authority has taken a decision referred to in paragraph 3, it shall communicate the reasons for that decision to the market surveillance authorities of the other Member States in which the AI system has been tested in accordance with the test plan.

Article 77

Powers of the authorities responsible for protecting fundamental rights

1. National public authorities or bodies responsible for supervising or enforcing obligations under Union law relating to the protection of fundamental rights, including the right to non-discrimination, with regard to the use of high-risk AI systems referred to in Annex III shall have the right to request and access any documentation created or maintained pursuant to this Regulation, in an accessible language and format, where access to such documentation is necessary for the effective performance of their mandates, within the limits of their jurisdiction. The relevant public authority or body shall inform the market surveillance authority of the relevant Member State of any such request.

2. By 2 November 2024, each Member State shall designate the public authorities or bodies referred to in paragraph 1 and include them in a list which it shall make publicly available. Member States shall notify that list to the Commission and the other Member States and shall keep it updated.

3. Where the documentation referred to in paragraph 1 is not sufficient to establish whether there has been a breach of the obligations under Union law relating to the protection of fundamental rights, the public authority or body referred to in paragraph 1 may submit a reasoned request to the market surveillance authority to organise testing of the high-risk AI system by technical means. The market surveillance authority shall organise the testing in close cooperation with the requesting public authority or body within a reasonable period of time after the request is submitted.

4. Any information or documentation obtained by national public authorities or bodies referred to in paragraph 1 of this Article pursuant to this Article shall be treated in accordance with the confidentiality obligations provided for in Article 78.

Article 78

Confidentiality

1. The Commission, market surveillance authorities, notified bodies and any other natural or legal person involved in the application of this Regulation, in accordance with Union or national law, shall respect the confidentiality of information and data obtained in the exercise of their tasks and activities in such a way as to protect, in particular:

a) intellectual and industrial property rights and confidential business information or trade secrets of a natural or legal person, including source code, except in the cases referred to in Article 5 of Directive (EU) 2016/943 of the European Parliament and of the Council [57];

(b) the effective application of this Regulation, in particular for the purposes of investigations, inspections or audits;

c) the interests of public and national security;

d) the development of criminal cases or administrative procedures;

(e) information classified under Union or national law.

2. Authorities involved in the application of this Regulation pursuant to paragraph 1 shall only request data that is strictly necessary for the assessment of the risk posed by AI systems and for the exercise of their powers under this Regulation and Regulation (EU) 2019/1020. They shall put in place appropriate and effective cybersecurity measures to protect the security and confidentiality of the information and data obtained, and shall erase the data collected as soon as it is no longer necessary for the purposes for which it was obtained, in accordance with applicable Union and national law.

3. Without prejudice to paragraphs 1 and 2, information exchanged on a confidential basis between competent national authorities or between competent national authorities and the Commission shall not be disclosed without prior consultation with the competent national authority of origin and the person responsible for deployment where law enforcement, border control, immigration or asylum authorities use high-risk AI systems referred to in points 1, 6 or 7 of Annex III and such disclosure would compromise public security and national security interests. This exchange of information shall not cover sensitive operational data relating to the activities of law enforcement, border control, immigration or asylum authorities.

Where law enforcement, immigration or asylum authorities are providers of high-risk AI systems referred to in points 1, 6 or 7 of Annex III, the technical documentation referred to in Annex IV shall remain within the premises of those authorities. Those authorities shall ensure that the market surveillance authorities referred to in Article 74(8) and (9), as appropriate, may, upon request, immediately access the documentation or obtain a copy of it. Access to such documentation or any copy thereof shall only be granted to staff of the market surveillance authority holding a security clearance of the appropriate level.

4. Paragraphs 1, 2 and 3 shall not affect the rights or obligations of the Commission, the Member States and their relevant authorities, nor the rights or obligations of notified bodies as regards the exchange of information and the dissemination of warnings, including in the context of cross-border cooperation, nor the obligations to provide information under the criminal law of the Member States incumbent on the parties concerned.

5. Where necessary and in accordance with the relevant provisions of international and trade agreements, the Commission and the Member States may exchange confidential information with regulatory authorities in third countries with which they have concluded bilateral or multilateral confidentiality agreements ensuring an appropriate level of confidentiality.

Article 79

Procedure applicable at national level to AI systems that present a risk

1. AI systems presenting a risk shall be understood as ‘products presenting a risk’ as defined in Article 3, point 19, of Regulation (EU) 2019/1020, to the extent that they present risks affecting the health, safety or fundamental rights of persons.

2. Where the market surveillance authority of a Member State has sufficient grounds to consider that an AI system presents a risk referred to in paragraph 1 of this Article, it shall carry out an assessment of the AI system concerned to verify its compliance with all the requirements and obligations set out in this Regulation. Particular attention should be paid to AI systems that present a risk to vulnerable groups. Where risks to fundamental rights are identified, the market surveillance authority shall also inform the relevant national public authorities or bodies referred to in Article 77(1) and shall fully cooperate with them. Relevant operators shall cooperate as necessary with the market surveillance authority and with the other national public authorities or bodies referred to in Article 77(1).

[57] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (OJ L 157 of 15.6.2016, p. 1).

Where, in the course of such assessment, the market surveillance authority or, where applicable, the market surveillance authority in cooperation with the national public authority referred to in Article 77(1), finds that the AI system does not comply with the requirements and obligations set out in this Regulation, it shall, without undue delay, require the relevant operator to take all appropriate corrective measures to bring the AI system into compliance with those requirements and obligations, to withdraw the AI system from the market or to recall it, within a period that that authority may determine and in any case within 15 working days at the latest or within such period as may be provided for in the relevant Union legislative harmonisation acts as appropriate.

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 of this paragraph.

3. Where the market surveillance authority considers that the non-compliance is not limited to its national territory, it shall inform the Commission and the other Member States without undue delay of the results of the assessment and of the measures it has requested the operator to take.

4. The operator shall ensure that all appropriate corrective measures are taken in relation to all affected AI systems that it has placed on the market in the Union.

5. Where the operator of an AI system fails to take appropriate corrective measures within the period referred to in paragraph 2, the market surveillance authority shall take all appropriate provisional measures to prohibit or restrict the placing on the market of the AI system on its national market or its putting into service, to withdraw the product or the stand-alone AI system from its national market or to recall it. That authority shall notify those measures without undue delay to the Commission and to the other Member States.

6. The notification referred to in paragraph 5 shall include all available details, in particular the information necessary for the identification of the non-compliant AI system, the origin of the AI system and the supply chain, the nature of the alleged non-compliance and the risk posed, the nature and duration of the national measures taken and the arguments put forward by the relevant operator. In particular, market surveillance authorities shall indicate whether the non-compliance is due to one or more of the following reasons:

(a) failure to comply with the prohibition on AI practices referred to in Article 5;

(b) failure by a high-risk AI system to comply with the requirements set out in Chapter III, Section 2;

(c) deficiencies in the harmonised standards or common specifications referred to in Articles 40 and 41 which confer the presumption of conformity;

d) failure to comply with Article 50.

7. Market surveillance authorities other than the market surveillance authority of the Member State that initiated the procedure shall, without undue delay, communicate to the Commission and to the other Member States any measure they take and any additional information at their disposal concerning the non-compliance of the AI system concerned and, in the event of disagreement with the notified national measure, their objections thereto.

8. If, within three months of receipt of the notification referred to in paragraph 5 of this Article, no objection is raised by any market surveillance authority of a Member State or by the Commission to a provisional measure taken by a market surveillance authority of another Member State, the measure shall be deemed to be justified. This is without prejudice to the procedural rights of the relevant operator under Article 18 of Regulation (EU) 2019/1020. The three-month period referred to in this paragraph shall be reduced to thirty days in the event of non-compliance with the prohibition of AI practices referred to in Article 5 of this Regulation.

9. Market surveillance authorities shall ensure that appropriate restrictive measures in respect of the product or AI system concerned, such as the withdrawal of the product or AI system from their market, are taken without undue delay.

Article 80

Procedure applicable to AI systems classified by the provider as not high risk in application of the Annex III

1. Where a market surveillance authority has sufficient grounds to consider that an AI system that the provider has classified as not high-risk pursuant to Article 6(3) is high-risk, that authority shall carry out an assessment of the AI system concerned as regards its classification as a high-risk AI system based on the conditions set out in Article 6(3) and the Commission guidelines.

2. Where, when carrying out such an assessment, the market surveillance authority finds that the AI system concerned is high-risk, it shall, without undue delay, require the relevant provider to take all measures necessary to ensure that the AI system complies with the requirements and obligations set out in this Regulation and to take appropriate corrective measures within a period that the market surveillance authority may determine.

3. Where the market surveillance authority considers that the use of the AI system concerned is not limited to its national territory, it shall inform the Commission and the other Member States without undue delay of the results of the assessment and of the measures it has required the provider to take.

4. The provider shall ensure that all necessary measures are taken to ensure that the AI system complies with the requirements and obligations set out in this Regulation. Where the provider of an affected AI system fails to take the necessary measures to ensure that it complies with those requirements and obligations within the period referred to in paragraph 2 of this Article, fines shall be imposed on the provider in accordance with Article 99.

5. The provider shall ensure that all appropriate corrective measures are taken for all affected AI systems that it has placed on the market throughout the Union.

6. Where the provider of the AI system concerned fails to take appropriate corrective measures within the period referred to in paragraph 2 of this Article, Article 79(5) to (9) shall apply.

7. Where, when carrying out the assessment pursuant to paragraph 1 of this Article, the market surveillance authority determines that the provider had wrongly classified the AI system as not high-risk in order to circumvent the application of the requirements set out in Chapter III, Section 2, fines shall be imposed on the provider in accordance with Article 99.

8. In exercising their powers to supervise the application of this Article, and in accordance with Article 11 of Regulation (EU) 2019/1020, market surveillance authorities may carry out appropriate checks, taking into account, in particular, the information stored in the EU database referred to in Article 71 of this Regulation.

Article 81

Union safeguard procedure

1. Where, within three months of receipt of the notification referred to in Article 79(5) or within 30 days in the event of non-compliance with the prohibition of AI practices referred to in Article 5, the market surveillance authority of a Member State raises objections to a measure taken by another market surveillance authority, or where the Commission considers that the measure is contrary to Union law, the Commission shall enter into consultations without undue delay with the market surveillance authority of the relevant Member State and the operator(s) and shall assess the national measure. On the basis of the results of that assessment, the Commission shall, within six months of the notification referred to in Article 79(5) or 60 days in the event of non-compliance with the prohibition of AI practices referred to in Article 5, decide whether the national measure is justified and shall notify its decision to the market surveillance authority of the Member State concerned. The Commission will also inform the other market surveillance authorities of its decision.

2. Where the Commission considers that the measure taken by the Member State concerned is justified, all Member States shall ensure that they take appropriate restrictive measures with regard to the AI system concerned, such as requiring the withdrawal of the AI system from their market without undue delay, and shall inform the Commission thereof. Where the Commission considers that the national measure is not justified, the Member State concerned shall withdraw the measure and inform the Commission thereof.

3. Where the national measure is considered to be justified and the non-compliance of the AI system is attributed to deficiencies in the harmonised standards or common specifications referred to in Articles 40 and 41 of this Regulation, the Commission shall apply the procedure provided for in Article 11 of Regulation (EU) No 1079/2008.either1025/2012.

Article 82

Compliant AI systems that present a risk

1. Where, after carrying out an assessment in accordance with Article 79 and consulting the national public authority referred to in Article 77(1), the market surveillance authority of a Member State concludes that a high-risk AI system, despite complying with this Regulation, nevertheless presents a risk to the health or safety of persons, to fundamental rights or to other aspects of the public interest, it shall require the operator concerned to take all appropriate measures to ensure that the AI system concerned no longer presents such a risk when it is placed on the market or put into service without undue delay, within a period that that authority may determine.

2. The provider or other relevant operator shall ensure that corrective measures are taken in respect of all affected AI systems that it has placed on the Union market within the period determined by the market surveillance authority of the Member State referred to in paragraph 1.

3. Member States shall immediately inform the Commission and the other Member States when a conclusion is reached pursuant to paragraph 1. The information provided shall include all available details, in particular the data necessary to detect the AI system concerned and to determine its origin and supply chain, the nature of the risk posed and the nature and duration of the national measures taken.

4. The Commission shall, without undue delay, enter into consultations with the Member States concerned and relevant operators and shall assess the national measures taken. Based on the results of this assessment, the Commission shall decide whether the measure is justified and, if appropriate, propose other appropriate measures.

5. The Commission shall immediately communicate its decision to the Member States concerned and to the relevant operators. It shall also inform the other Member States.

Article 83

Formal non-compliance

1. Where the market surveillance authority of a Member State finds one of the following situations, it shall require the supplier concerned to remedy the non-compliance in question within a period which the market surveillance authority may determine:

a) the CE marking has been affixed in breach of Article 48;

b) the CE marking has not been affixed;

(c) the EU declaration has not been drawn up in accordance with Article 47;

(d) the EU declaration has not been drawn up correctly in accordance with Article 47;

(e) the registration in the EU database in accordance with Article 71 has not been carried out;

f) where applicable, an authorized representative has not been appointed;

g) no technical documentation is available.

2. If the non-compliance referred to in paragraph 1 persists, the market surveillance authority of the Member State concerned shall take appropriate and proportionate measures to restrict or prohibit the placing on the market of the high-risk AI system or to ensure that it is recalled or withdrawn from the market without delay.

Article 84

Support structures for EU AI testing

1. The Commission shall designate one or more Union AI testing support structures to carry out the activities listed in Article 21(6) of Regulation (EU) 2019/1020 in the field of AI.

2. Without prejudice to the activities referred to in paragraph 1, the Union AI testing support structures shall also provide independent technical or scientific advice at the request of the AI Council, the Commission or market surveillance authorities.

SECTION 4

Ways of appeal

Article 85

Right to lodge a complaint with a market surveillance authority

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

In accordance with Regulation (EU) 2019/1020, such complaints will be taken into account when carrying out market surveillance activities and will be handled in accordance with specific procedures established for this purpose by the market surveillance authorities.

Article 86

Right to explanation of decisions taken individually

1. Any person who is affected by a decision taken by the deployer on the basis of the output results of a high-risk AI system listed in Annex III, with the exception of those systems listed in point 2 thereof, and which produces legal effects or substantially affects him or her, such that he or she considers that it has a detrimental effect on his or her health, safety or fundamental rights, shall have the right to obtain from the deployer clear and meaningful explanations about the role that the AI system has played in the decision-making process and the main elements of the decision taken.

2. Paragraph 1 shall not apply to the use of AI systems for which there are exceptions or restrictions to the obligation provided for in that paragraph arising from Union or national law in accordance with Union law.

3. This Article shall apply only to the extent that the right referred to in paragraph 1 is not otherwise provided for by Union law.

Article 87

Reporting infringements and protection of whistleblowers

Directive (EU) 2019/1937 shall apply to the reporting of infringements of this Regulation and to the protection of persons who report such infringements.

SECTION 5

Supervision, investigation, compliance and monitoring of general-purpose AI model providers

Article 88

Compliance with obligations for general-purpose AI model providers

1. The Commission shall have exclusive powers to monitor and enforce compliance with Chapter V, taking into account the procedural guarantees provided for in Article 94. The Commission should entrust the execution of these tasks to the IA Office, without prejudice to the organisational powers of the Commission and the distribution of powers between the Member States and the Union under the Treaties.

2. Without prejudice to Article 75(3), market surveillance authorities may request the Commission to exercise the powers provided for in this Section where necessary and proportionate to assist the performance of the activities falling within their competence under this Regulation.

Article 89

Follow-up measures

1. In order to carry out the tasks conferred on it by this Section, the AI Office may take the necessary measures to monitor the effective implementation and enforcement of this Regulation by providers of general-purpose AI models, including their compliance with approved codes of good practice.

2. Subsequent suppliers shall have the right to lodge complaints alleging infringements of this Regulation. Complaints shall be duly motivated and shall indicate at least:

a) the point of contact of the provider of the general-purpose AI model in question;

(b) a description of the facts, the provisions of this Regulation affected and the reasons why the downstream provider considers that the provider of the general-purpose AI model concerned has infringed this Regulation;

c) any other information that the subsequent provider submitting the complaint considers relevant, such as, where appropriate, information that it has collected on its own initiative.

Article 90

Warnings from the group of scientific experts on systemic risks

1. The scientific expert group may provide qualified alerts to the AI Office when it has reason to suspect that:

(a) a general-purpose AI model poses a specific risk recognisable at Union level, or

(b) a general-purpose AI model meets the conditions referred to in Article 51.

2. Following receipt of such a qualified alert, the Commission may, through the AI Office and after having informed the AI Council, exercise the powers provided for in this Section in order to assess the matter. The AI Office shall inform the AI Council of any measure taken in accordance with Articles 91 to 94.

3. Qualified alerts must be duly justified and indicate, as a minimum:

a) the point of contact of the provider of the general-purpose AI model with systemic risk in question;

b) a description of the facts and the reasons why the scientific expert group is providing the alert;

(c) any other information that the scientific expert group considers relevant, such as, where appropriate, information it has collected on its own initiative.

Article 91

Powers to request documentation and information

1. The Commission may request the provider of the general-purpose AI model concerned to provide the documentation prepared by the provider in accordance with Articles 53 and 55, or any other information that is necessary to assess the provider's compliance with this Regulation.

2. Before sending the request for information, the AI Office may engage in a structured dialogue with the provider of the general-purpose AI model.

3. Where the scientific expert group submits a duly reasoned request, the Commission may address a request for information to the provider of a general-purpose AI model if access to such information is necessary and proportionate for the scientific expert group to carry out its tasks under Article 68(2).

4. The request for information shall indicate the legal basis and purpose of the request, specify what information is required, set the time limit within which the information must be provided and indicate the fines established in Article 101 for providing incorrect, incomplete or misleading information.

5. The general-purpose AI model provider concerned, or its representative, shall provide the requested information. In the case of legal persons, companies or businesses, or where the provider does not have legal personality, persons authorised by law or by their bylaws to represent them shall provide the requested information on behalf of the general-purpose AI model provider concerned. Duly authorised lawyers may provide the information on behalf of their clients. The clients shall, however, remain fully liable if the information provided is incomplete, incorrect or misleading.

Article 92

Powers to carry out evaluations

1. The AI Office, after consulting the AI Council, may carry out assessments of the general-purpose AI model in question in order to:

(a) assess whether the supplier complies with its obligations under this Regulation, where the information collected pursuant to Article 91 is insufficient, or

(b) investigate Union-wide systemic risks of general-purpose AI models with systemic risk, in particular following a qualified alert from the scientific expert group in accordance with point (a) of Article 90(1).

2. The Commission may decide to appoint independent experts to carry out the assessments on its behalf, including scientific experts from the group established in accordance with Article 68. The independent experts appointed to carry out these tasks shall comply with the criteria set out in Article 68(2).

3. For the purposes of paragraph 1, the Commission may request access to the general-purpose AI model in question through APIs or other appropriate technical means and tools, such as source code.

4. The request for access shall indicate the legal basis, the purpose and the reasons for the request, and shall set out the period during which access must be provided and the fines established in Article 101 for failure to provide it.

5. The interested general-purpose AI model providers or their representative shall provide the requested information. In the case of legal persons, companies or businesses, or when the provider does not have legal personality, the persons empowered by law or by their statutes to represent them, shall facilitate the requested access on behalf of the interested general-purpose AI model provider.

6. The Commission shall adopt implementing acts laying down the detailed modalities and conditions of the evaluations, including the detailed arrangements for the involvement of independent experts and the procedure for their selection. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

7. Before requesting access to the relevant general-purpose AI model, the AI Office may engage in a structured dialogue with the provider of the general-purpose AI model to gather further information on the model's internal testing, internal safeguards to prevent systemic risks, and other internal procedures and measures the provider has taken to mitigate such risks.

Article 93

Powers to request the adoption of measures

1. Where necessary and appropriate, the Commission may require suppliers to:

(a) take appropriate measures to comply with the obligations set out in Articles 53 and 54;

(b) implement risk mitigation measures where the assessment carried out in accordance with Article 92 indicates that there are serious and well-founded reasons for concern about the existence of a systemic risk at Union level;

c) restrict the marketing of the model, withdraw it or recover it.

2. Before requesting action, the AI Office may engage in a structured dialogue with the provider of the general-purpose AI model.

3. If, during the structured dialogue referred to in paragraph 2, the provider of the general-purpose AI model with systemic risk commits to take mitigation measures to address a systemic risk at Union level, the Commission may, by means of a decision, make those commitments binding and declare that there are no longer grounds for action.

Article 94

Procedural guarantees for economic operators of the general-purpose AI model

Article 18 of Regulation (EU) 2019/1020 shall applymutatis mutandisto providers of the general-purpose AI model, without prejudice to the more specific procedural safeguards provided for in this Regulation.

CHAPTER X

CODES OF CONDUCT AND GUIDELINES

Article 95

Codes of conduct for the voluntary application of specific requirements

1. The AI Office and Member States shall encourage and facilitate the development of codes of conduct, with appropriate governance mechanisms, aimed at encouraging the voluntary application of some or all of the requirements set out in Chapter III, Section 2, to non-high-risk AI systems, taking into account available technical solutions and industry best practices enabling the implementation of those requirements.

2. The AI Office and Member States shall facilitate the development of codes of conduct regarding the voluntary implementation, including by deployers, of specific requirements for all AI systems, based on clear objectives and key performance indicators to measure the achievement of those objectives, including, but not limited to, elements such as:

(a) the applicable elements set out in the Union Ethical Guidelines for Trustworthy AI;

(b) assessing and minimising the impacts of AI systems on environmental sustainability, including with regard to energy-efficient programming and techniques for efficiently designing, training and using AI;

(c) promoting AI literacy, in particular for those involved in the development, operation and use of AI;

(d) facilitating inclusive and diverse design of AI systems, for example by creating inclusive and diverse development teams and promoting stakeholder participation in that process;

(e) the assessment and prevention of harm caused by AI systems to vulnerable persons or groups of vulnerable persons, including with regard to accessibility for persons with disabilities, as well as gender equality.

3. Codes of conduct may be developed by providers or deployers of particular AI systems, their representative organisations or both, including with the involvement of any interested parties and their representative organisations, such as civil society organisations and academia. Codes of conduct may cover one or more AI systems depending on the similarity of the intended purpose of the different systems.

4. The AI Office and Member States shall take into account the specific interests and needs of SMEs, including start-ups, when encouraging and facilitating the development of codes of conduct.

Article 96

Commission guidelines on the application of this Regulation

1. The Commission shall draw up guidelines on the practical application of this Regulation and in particular on:

(a) the application of the requirements and obligations referred to in Articles 8 to 15 and Article 25;

b) the prohibited practices referred to in Article 5;

c) the practical application of the provisions relating to substantial modifications;

(d) the practical application of the transparency obligations set out in Article 50;

(e) detailed information on the relationship between this Regulation and the list of Union harmonisation legislative acts listed in Annex I, as well as other relevant provisions of Union law, including as regards consistency in their application;

(f) the application of the definition of AI system set out in Article 3, point 1.

When publishing these guidelines, the Commission will pay particular attention to the needs of SMEs, including start-ups, local public authorities and sectors most likely to be affected by this Regulation.

The guidelines referred to in the first subparagraph of this paragraph shall take due account of the generally recognised state of the art in the field of AI as well as relevant harmonised standards and common specifications referred to in Articles 40 and 41, or harmonised standards or technical specifications established pursuant to Union harmonisation law.

2. At the request of Member States or the AI Office, or on its own initiative, the Commission shall update previously adopted guidelines where deemed necessary.

CHAPTER XI

DELEGATION OF POWERS AND COMMITTEE PROCEDURE

Article 97

Exercise of delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 6(6), Article 7, Article 7(1) and (3), Article 11(3), Article 43(5) and (6), Article 47(5), Article 51(3), Article 52(4) and Article 53(5) and (6) shall be conferred on the Commission for a period of five years from 1 August 2024. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

3. The delegation of power referred to in Article 6(6) and (7), Article 7(1) and (3), Article 11(3), Article 43(5) and (6), Article 47(5), Article 51(3), Article 52(4) and Article 53(5) and (6) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect on the day following that of its publication in the European Parliament.Official Journal of the European Unionor at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Article 6(6) or (7), Article 7(1) or (3), Article 11(3), Article 43(5) or (6), Article 47(5), Article 51(3), Article 52(4) or Article 53(5) or (6) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Article 98

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 1999/2002.
n.either182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) shall apply.
n.either182/2011.

CHAPTER XII

SANCTIONS

Article 99

Sanctions

1. Subject to the conditions laid down in this Regulation, Member States shall lay down the system of penalties and other enforcement measures, such as warnings or non-pecuniary measures, applicable to infringements of this Regulation committed by operators and shall take all necessary measures to ensure that they are applied in an appropriate and effective manner, taking into account the guidelines issued by the Commission pursuant to Article 96. Such penalties shall be effective, proportionate and dissuasive. They shall take into account the interests of SMEs, including start-ups, as well as their economic viability.

2. Member States shall communicate to the Commission without delay and at the latest on the date of application the rules concerning the penalties and other enforcement measures referred to in paragraph 1 and shall inform it without delay of any amendment to those rules.

3. Failure to comply with the prohibition on AI practices referred to in Article 5 shall be subject to administrative fines of up to EUR 35 000 000 or, if the offender is an undertaking, up to 7 % of its total worldwide turnover for the preceding financial year, whichever is higher.

4. Failure to comply with any of the following provisions in relation to operators or notified bodies other than those referred to in Article 5 shall be subject to administrative fines of up to EUR 15 000 000 or, if the offender is an undertaking, up to 3 % of its total worldwide turnover for the preceding financial year, whichever is higher:

(a) the obligations of suppliers pursuant to Article 16;

(b) the obligations of authorised representatives pursuant to Article 22;

(c) the obligations of importers under Article 23;

(d) the obligations of distributors under Article 24;

(e) the obligations of those responsible for deployment under Article 26;

(f) the requirements and obligations of notified bodies pursuant to Article 31, Article 33(1), (3) and (4) or Article 34;

(g) the transparency obligations of providers and deployers pursuant to Article 50.

5. The submission of inaccurate, incomplete or misleading information to notified bodies or to the competent national authorities in response to a request shall be subject to administrative fines of up to EUR 7 500 000 or, if the offender is an undertaking, up to 1 % of the total worldwide turnover for the previous financial year, whichever is higher.

6. In the case of SMEs, including start-ups, each of the fines referred to in this article may be for the percentage or the amount referred to in paragraphs 3, 4 and 5, whichever is lower.

7. When deciding whether to impose an administrative fine and its amount in each specific case, all the relevant circumstances of the situation in question shall be taken into account and, where appropriate, the following shall be taken into account:

(a) the nature, severity and duration of the infringement and its consequences, taking into account the purpose of the AI system and, where applicable, the number of persons affected and the level of harm suffered;

(b) whether other market surveillance authorities have already imposed administrative fines on the same operator for the same infringement;

(c) if other authorities have already imposed administrative fines on the same operator for infringements of other national or Union legislative acts, where such infringements arise from the same activity or omission constituting a relevant infringement of this Regulation;

(d) the size, annual turnover and market share of the operator committing the infringement;

(e) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits obtained or losses avoided, directly or indirectly, through the infringement;

(f) the degree of cooperation with the competent national authorities in order to remedy the infringement and mitigate its potential adverse effects;

g) the degree of responsibility of the operator, taking into account the technical and organisational measures applied by the operator;

(h) the manner in which the competent national authorities became aware of the infringement, in particular whether the operator notified the infringement and, if so, to what extent;

i) the intentionality or negligence of the infringement;

j) the actions taken by the operator to mitigate the damage suffered by the affected persons.

8. Each Member State shall lay down rules determining the extent to which administrative fines may be imposed on public authorities and bodies established in that Member State.

9. Depending on the legal system of the Member States, the rules on administrative fines may be applied in such a way that fines are imposed by competent national courts or other bodies, as appropriate in those Member States. The application of those rules in those Member States shall have equivalent effect.

10. The exercise of powers under this Article shall be subject to appropriate procedural guarantees in accordance with Union and national law, including effective judicial protection and due process.

11. Member States shall report annually to the Commission on administrative fines imposed during that year in accordance with this Article and on any related litigation or judicial proceedings.

Article 100

Administrative fines imposed on institutions, bodies and agencies of the European Union

1. The European Data Protection Supervisor may impose administrative fines on Union institutions, bodies, offices and agencies falling within the scope of this Regulation. When deciding on the imposition of an administrative fine and its amount in each individual case, all relevant circumstances of the situation in question shall be taken into account and due account shall be taken of the following:

(a) the nature, severity and duration of the infringement and its consequences, taking into account the purpose of the AI system concerned, as well as, where applicable, the number of persons affected and the level of harm suffered by them;

(b) the degree of responsibility of the Union institution, body, office or agency, taking into account the technical and organisational measures applied;

(c) the actions taken by the Union institution, body, office or agency to mitigate the harm suffered by the persons concerned;

(d) the extent of cooperation with the European Data Protection Supervisor in order to remedy the breach and mitigate its potential adverse effects, including compliance with any measures that the European Data Protection Supervisor has previously ordered against the Union institution, body, office or agency concerned in relation to the same matter;

(e) any previous similar infringement committed by the Union institution, body, office or agency;

(f) the manner in which the European Data Protection Supervisor became aware of the breach, in particular whether the Union institution, body, office or agency notified the European Data Protection Supervisor of the breach and, if so, to what extent;

(g) the annual budget of the Union institution, body, office or agency.

2. Failure to comply with the prohibition on AI practices referred to in Article 5 shall be subject to administrative fines of up to EUR 1 500 000.

3. Failure by the AI system to comply with any of the requirements or obligations set out in this Regulation, other than those provided for in Article 5, shall be subject to administrative fines of up to EUR 750 000.

4. Before taking any decision under this Article, the European Data Protection Supervisor shall give the Union institution, body, office or agency subject to the procedure conducted by the European Data Protection Supervisor the opportunity to be heard with regard to the alleged infringement. The European Data Protection Supervisor shall base his or her decisions solely on the elements and circumstances on which the parties concerned have been able to make representations. Complainants, if any, shall be closely involved in the procedure.

5. The parties' rights of defence shall be fully guaranteed during the proceedings. They shall have the right to access the file of the European Data Protection Supervisor, without prejudice to the legitimate interest of individuals and companies in the protection of their personal data or trade secrets.

6. The proceeds from fines imposed pursuant to this Article shall contribute to the general budget of the Union. Fines shall not affect the effective functioning of the Union institution, body, office or agency penalised.

7. The European Data Protection Supervisor shall report annually to the Commission on any administrative fines imposed pursuant to this Article and on any litigation or legal proceedings initiated by him or her.

Article 101

Fines for providers of general-purpose AI models

1. The Commission may impose fines on providers of general-purpose AI models not exceeding 3 % of their total annual global turnover for the preceding financial year or EUR 15 000 000, whichever is higher, where the Commission finds that, intentionally or negligently:

a) infringed the relevant provisions of this Regulation;

(b) have failed to respond to a request for information or documents pursuant to Article 91, or have provided inaccurate, incomplete or misleading information;

c) failed to comply with a measure requested under Article 93;

(d) did not provide the Commission with access to the general-purpose AI model or the general-purpose AI model with systemic risk for an assessment to be carried out pursuant to Article 92.

When setting the amount of the fine or periodic penalty payment, consideration shall be given to the nature, gravity and duration of the infringement, with due regard to the principles of proportionality and adequacy. The Commission shall also take into account the commitments made in accordance with Article 93(3) and in the relevant codes of good practice provided for in Article 56.

2. Before adopting a decision pursuant to paragraph 1, the Commission shall communicate its preliminary findings to the provider of the general-purpose AI model or the AI model and give it the opportunity to be heard.

3. Fines imposed pursuant to this Article shall be effective, proportionate and dissuasive.

4. Information on fines imposed under this Article shall also be communicated to the IA Board, as appropriate.

5. The Court of Justice of the European Union shall have full jurisdiction to review decisions imposing a fine adopted by the Commission pursuant to this Article. It may annul, reduce or increase the amount of the fine imposed.

6. The Commission shall adopt implementing acts containing detailed provisions and procedural safeguards for the procedures with a view to the possible adoption of decisions pursuant to paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

CHAPTER XIII

FINAL PROVISIONS

Article 102

Amendment to Regulation (EC) No.either300/2008

In Article 4(3) of Regulation (EC) No.either300/2008, the following paragraph is added:

"When adopting detailed measures concerning the technical specifications and procedures for approval and use of security equipment in relation to artificial intelligence systems within the meaning of Regulation (EU) 2024/1689 of the European Parliament and of the Council (*), the requirements set out in Chapter III, Section 2 of that Regulation shall be taken into account.

(*) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 establishing harmonised rules on artificial intelligence and amending Regulations (EC) No 1689/2008 and (EC) No 1689/2009.either300/2008, (EU) n.either167/2013, (EU) n.either168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Regulation) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Article 103

Amendment to Regulation (EU) No.either167/2013

In Article 17(5) of Regulation (EU) No.either167/2013, the following paragraph is added:

"When adopting delegated acts pursuant to the first subparagraph relating to artificial intelligence systems that are security components within the meaning of Regulation (EU) 2024/1689 of the European Parliament and of the Council (*), account shall be taken of the requirements set out in Chapter III, Section 2 of that Regulation.

(*) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 establishing harmonised rules on artificial intelligence and amending Regulations (EC) No 1689/2008 and (EC) No 1689/2009.either300/2008, (EU) n.either167/2013, (EU) n.either168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Regulation) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Article 104

Amendment to Regulation (EU) No.either168/2013

In Article 22(5) of Regulation (EU) No.either168/2013, the following paragraph is added:

"When adopting delegated acts pursuant to the first subparagraph relating to artificial intelligence systems that are security components within the meaning of Regulation (EU) 2024/1689 of the European Parliament and of the Council (*), account shall be taken of the requirements set out in Chapter III, Section 2 of that Regulation.

(*) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 establishing harmonised rules on artificial intelligence and amending Regulations (EC) No 1689/2008 and (EC) No 1689/2009.either300/2008, (EU) n.either167/2013, (EU) n.either168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Regulation) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Article 105

Amendment to Directive 2014/90/EU

In Article 8 of Directive 2014/90/EU, the following paragraph is added:

«5. In the case of artificial intelligence systems that are security components within the meaning of the Regulation (EU) 2024/1689 of the European Parliament and of the Council (*), the Commission shall take into account the requirements set out in Chapter III, Section 2 of that Regulation when carrying out its activities pursuant to paragraph 1 and when adopting technical specifications and testing standards in accordance with paragraphs 2 and 3.

(*) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 establishing harmonised rules on artificial intelligence and amending Regulations (EC) No 1689/2008 and (EC) No 1689/2009.either300/2008, (EU) n.either167/2013, (EU) n.either168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Regulation) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Article 106

Amendment to Directive (EU) 2016/797

In Article 5 of Directive (EU) 2016/797, the following paragraph is added:

«12. By adopting delegated acts pursuant to paragraph 1 and implementing acts pursuant to paragraph 11 concerning
For artificial intelligence systems that are security components within the meaning of Regulation (EU) 2024/1689 of the European Parliament and of the Council (*), the requirements set out in Chapter III, Section 2 of that Regulation shall be taken into account.

(*) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 establishing harmonised rules on artificial intelligence and amending Regulations (EC) No 1689/2008 and (EC) No 1689/2009.either300/2008, (EU) n.either167/2013, (EU) n.either168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Regulation) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Article 107

Amendment to Regulation (EU) 2018/858

In Article 5 of Regulation (EU) 2018/858, the following paragraph is added:

«4. When adopting delegated acts pursuant to paragraph 3 relating to artificial intelligence systems that are safety components within the meaning of Regulation (EU) 2024/... of the European Parliament and of the Council (*), the requirements set out in Chapter III, Section 2 of that Regulation shall be taken into account.

(*) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 establishing harmonised rules on artificial intelligence and amending Regulations (EC) No 1689/2008 and (EC) No 1689/2009.either300/2008, (EU) n.either167/2013, (EU) n.either168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Regulation) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Article 108

Amendment to Regulation (EU) 2018/1139

Regulation (EU) 2018/1139 is amended as follows:

1) In Article 17, the following paragraph is added:

«3. Without prejudice to paragraph 2, when adopting implementing acts pursuant to paragraph 1 relating to For artificial intelligence systems that are security components within the meaning of Regulation (EU) 2024/1689 of the European Parliament and of the Council (*), the requirements set out in Chapter III, Section 2 of that Regulation shall be taken into account.

(*) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 establishing harmonised rules on artificial intelligence and amending Regulations (EC) No 1689/2008 and (EC) No 1689/2009. either300/2008, (EU) n.either167/2013, (EU) n.either168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Regulation) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

2) In Article 19, the following paragraph is added:

«4. By adopting delegated acts pursuant to paragraphs 1 and 2 concerning artificial intelligence systems that are safety components within the meaning of Regulation (EU) 2024/1689, the requirements set out in Chapter III, Section 2 of that Regulation shall be taken into account.».

3) In Article 43, the following paragraph is added:

«4. When adopting implementing acts pursuant to paragraph 1 relating to artificial intelligence systems that are safety components within the meaning of Regulation (EU) 2024/1689, the requirements set out in Chapter III, Section 2 of that Regulation shall be taken into account.».

4) In Article 47, the following paragraph is added:

«3. By adopting delegated acts pursuant to paragraphs 1 and 2 concerning artificial intelligence systems that are safety components within the meaning of Regulation (EU) 2024/1689, the requirements set out in Chapter III, Section 2 of that Regulation shall be taken into account.».

5) In Article 57, the following paragraph is added:

"When adopting those implementing acts relating to artificial intelligence systems that are security components within the meaning of Regulation (EU) 2024/1689, account shall be taken of the requirements set out in Chapter III, Section 2 of that Regulation."

6) In Article 58, the following paragraph is added:

«3. By adopting delegated acts pursuant to paragraphs 1 and 2 concerning artificial intelligence systems that are safety components within the meaning of Regulation (EU) 2024/1689, the requirements set out in Chapter III, Section 2 of that Regulation shall be taken into account.».

Article 109

Amendment to Regulation (EU) 2019/2144

In Article 11 of Regulation (EU) 2019/2144, the following paragraph is added:

«3. When adopting implementing acts pursuant to paragraph 2 relating to artificial intelligence systems that are safety components within the meaning of Regulation (EU) 2024/1689 of the European Parliament and of the Council (*), the requirements set out in Chapter III, Section 2 of that Regulation shall be taken into account.

(*) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 establishing harmonised rules on artificial intelligence and amending Regulations (EC) No 1689/2008 and (EC) No 1689/2009.either300/2008, (EU) n.either167/2013, (EU) n.either168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Regulation) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Article 110

Amendment to Directive (EU) 2020/1828

In Annex I of Directive (EU) 2020/1828 of the European Parliament and of the Council [58] the following point is added:

"68) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 1689 laying down rules harmonised measures in the field of artificial intelligence and amending Regulations (EC) No.either300/2008, (EU) n.either 167/2013, (EU) n.either168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Regulation) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Article 111

AI systems already introduced to the market or put into service and general-purpose AI models already introduced into the market

1. Without prejudice to the application of Article 5 in accordance with point (a) of Article 113(3), AI systems that are components of large-scale computing systems established pursuant to the legislative acts listed in Annex X that are placed on the market or put into service before 2 August 2027 shall comply with this Regulation by 31 December 2030.

The requirements set out in this Regulation shall be taken into account in the assessment of each large-scale IT system established pursuant to the legal acts listed in Annex X carried out in accordance with those legal acts and where those legal acts have been replaced or amended.

2. Without prejudice to the application of Article 5 pursuant to point (a) of Article 113(3), this Regulation shall apply to operators of high-risk AI systems, other than those referred to in paragraph 1 of this Article, that have been placed on the market or put into service before 2 August 2026 only if, from that date, those systems undergo significant changes to their design. In any case, providers and those responsible for the deployment of high-risk AI systems intended for use by public authorities shall take the necessary measures to comply with the requirements and obligations of this Regulation by 2 August 2030.

3. Providers of general-purpose AI models that have been placed on the market before 2 August 2025 shall take the necessary measures to comply with the obligations set out in this Regulation by 2 August 2027.

[58] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409, 4.12.2020, p. 1).

Article 112

Evaluation and review

1. The Commission shall assess the need to amend the list in Annex III and the list of prohibited AI practices provided for in Article 5 once a year from the entry into force of this Regulation until the end of the period of delegation of powers provided for in Article 97. The Commission shall present the conclusions of that assessment to the European Parliament and to the Council.

2. By 2 August 2028, and every four years thereafter, the Commission shall assess the following points and report to the European Parliament and the Council:

(a) the need to expand the areas listed in Annex III or to add new areas;

(b) the need to amend the list of AI systems requiring additional transparency measures pursuant to Article 50;

c) the need to improve the effectiveness of the oversight and governance system.

3. By 2 August 2029, and every four years thereafter, the Commission shall submit to the European Parliament and to the Council a report on the evaluation and review of this Regulation. The report shall include an assessment of the enforcement structure and of the possible need for a Union agency to address the deficiencies identified. Based on its findings, that report shall be accompanied, where appropriate, by a proposal for amending this Regulation. The reports shall be made public.

4. In the reports referred to in paragraph 2, particular attention shall be paid to the following:

(a) the state of the financial, technical and human resources of the competent national authorities to carry out effectively the tasks assigned to them under this Regulation;

(b) the state of sanctions, in particular administrative fines referred to in Article 99(1), applied by Member States to infringements of the provisions of this Regulation;

(c) the harmonised standards adopted and common specifications developed in support of this Regulation;

(d) the number of companies entering the market after the start of application of this Regulation, including the number of SMEs.

5. By 2 August 2028, the Commission shall assess the functioning of the AI Office, whether it has been given sufficient powers and competences to carry out its tasks, and whether it would be relevant and necessary for the proper application and enforcement of this Regulation to enhance the AI Office and its implementing powers, as well as to increase its resources. The Commission shall submit a report on its assessment to the European Parliament and to the Council.

6. By 2 August 2028 and every four years thereafter, the Commission shall present a report on the review of progress in the development of standardisation documents on the energy-efficient development of general-purpose AI models and assess the need for additional measures or actions, including binding measures or actions. This report shall be submitted to the European Parliament and the Council and made public.

7. By 2 August 2028 and every three years thereafter, the Commission shall assess the impact and effectiveness of the voluntary codes of conduct in promoting the application of the requirements set out in Chapter III, Section 2 to AI systems that are not high-risk and, where appropriate, of other additional requirements applicable to AI systems that are not high-risk AI systems, such as requirements relating to environmental sustainability.

8. For the purposes of paragraphs 1 to 7, the IA Board, the Member States and the national competent authorities shall provide information to the Commission, upon request and without undue delay.

9. When carrying out the evaluations and reviews referred to in paragraphs 1 to 7, the Commission shall take into account the positions and conclusions of the IA Board, the European Parliament, the Council and other relevant bodies or sources.

10. The Commission shall, where necessary, submit appropriate proposals for amending this Regulation, in particular taking into account technological developments and the impact of AI systems on health and safety and fundamental rights, and in light of developments in the information society.

11. In order to guide the assessments and reviews referred to in paragraphs 1 to 7 of this Article, the AI Office shall be responsible for developing an objective and participatory methodology for the assessment of risk levels based on the criteria set out in the relevant Articles and the inclusion of new systems in:

(a) the list set out in Annex III, including the extension of existing areas or the inclusion of new areas in that Annex;

b) the list of prohibited practices set out in Article 5, and

(c) the list of AI systems requiring additional transparency measures pursuant to Article 50.

12. Amendments to this Regulation pursuant to paragraph 10, or relevant delegated or implementing acts, affecting sectoral Union harmonisation legislative acts listed in Section B of Annex I shall take into account the regulatory specificities of each sector and the governance, conformity assessment and enforcement mechanisms in place, as well as the authorities established therein.

13. By 2 August 2031, the Commission shall evaluate the implementation of this Regulation and report thereon to the European Parliament, the Council and the European Economic and Social Committee, taking into account the first years of application of this Regulation. On the basis of its findings, that report shall be accompanied, where appropriate, by a proposal for amending this Regulation as regards the implementation structure and the need for a Union agency to address the deficiencies identified.

Article 113

Entry into force and application

This Regulation shall enter into force on the twentieth day following its publication in theOfficial Journal of the European

Union. It will be applicable from August 2, 2026. However:

(a) Chapters I and II shall apply from 2 February 2025;

(b) Chapter III, Section 4, Chapter V, Chapter VII and Chapter XII and Article 78 shall apply from 2 August 2025, with the exception of Article 101;

(c) Article 6(1) and the corresponding obligations of this Regulation shall apply from 2 August 2027.

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

Done at Brussels, 13 June 2024.

By the European Parliament	By the Council
The President	The President
R. METSOLA	Mr. MICHEL

ANNEX I

List of Union harmonisation legislative acts

Section A — List of Union harmonisation legislative acts based on the new legislative framework

1. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery and amending Directive 95/16/EC (OJ L 157, 9.6.2006, p. 24)

2. Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (OJ L 170, 30.6.2009, p. 1)

3. Directive 2013/53/EU of the European Parliament and of the Council of 20 November 2013 on recreational crafts and personal watercraft and repealing Directive 94/25/EC (OJ L 354, 28.12.2013, p. 90)

4. Directive 2014/33/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to lifts and safety components for lifts (OJ L 96, 29.3.2014, p. 251)

5. Directive 2014/34/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to equipment and protective systems intended for use in potentially explosive atmospheres (OJ L 96, 29.3.2014, p. 309)

6. Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the marketing of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014, p. 62)

7. Directive 2014/68/EU of the European Parliament and of the Council of 15 May 2014 on the harmonisation of the laws of the Member States relating to the marketing of pressure equipment (OJ L 189, 27.6.2014, p. 164)

8. Regulation (EU) 2016/424 of the European Parliament and of the Council of 9 March 2016 on cableway installations and repealing Directive 2000/9/EC (OJ L 81, 31.3.2016, p. 1)

9. Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC (OJ L 81, 31.3.2016, p. 51)

10. Regulation (EU) 2016/426 of the European Parliament and of the Council of 9 March 2016 on appliances burning gaseous fuels and repealing Directive 2009/142/EC (OJ L 81, 31.3.2016, p. 99)

11. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 1018/2009 and Regulation (EC) No 1018/2009.either178/2002 and Regulation (EC) No.either1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1)

12. Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on diagnostic medical devicesin vitroand repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176)

Section B — List of other Union harmonisation legislative acts

13. Regulation (EC) No.either300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules on civil aviation security and repealing Regulation (EC) No 300/2008.either2320/2002 (OJ L 97, 9.4.2008, p. 72)

14. Regulation (EU) No.either168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval of two- or three-wheeled vehicles and quadricycles and the market surveillance of such vehicles (OJ L 60, 2.3.2013, p. 52)

15. Regulation (EU) No.either167/2013 of the European Parliament and of the Council of 5 February 2013 on type-approval of agricultural or forestry vehicles and on market surveillance of such vehicles (OJ L 60, 2.3.2013, p. 1)

16. Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment, and repealing Council Directive 96/98/EC (OJ L 257, 28.8.2014, p. 146)

17. Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on interoperability of the railway system within the European Union (OJ L 138, 26.5.2016, p. 44)

18. Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on approval and market surveillance of motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 189/2018 and (EC) No 189/201 … and (EC) No 189/2018 and (EC) No 189/2018 and (EC) No 189/2018 and (EC) No 189/2018 and (EC) No 189/2018 and (EC) No 189/2018 and (EC) n.either715/2007 and (EC) No.either595/2009 and repealing Directive 2007/46/EC (OJ L 151, 14.6.2018, p. 1)

19. Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, with regard to their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 1018/2009 of the European Parliament and of the Council. n.either78/2009, (EC) No.either79/2009 and (EC) No.either661/2009 of the European Parliament and of the Council and Regulations (EC) n.either631/2009, (EU) n.either406/2010, (EU) n.either672/2010, (EU) n.either1003/2010, (EU) n.either1005/2010, (EU) n.either1008/2010, (EU) n.either1009/2010, (EU) n.either19/2011, (EU) n.either109/2011, (EU) n.either458/2011, (EU) n.either65/2012, (EU) n.either130/2012, (EU) n.either347/2012, (EU) n.either351/2012, (EU) n.either1230/2012 and (EU) 2015/166 of the Commission (OJ L 325, 16.12.2019, p. 1)

20. Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 1139/2018 and (EC) No 1139/2018.either2111/2005, (EC) No.either1008/2008, (EU) n.either996/2010 and (EU) n.either376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council and Regulations (EC) No. either552/2004 and (EC) No.either216/2008 of the European Parliament and of the Council and Regulation (EEC) No.either 3922/91 of the Council (OJ L 212, 22.8.2018, p. 1), insofar as it affects the design, production and placing on the market of aircraft referred to in Article 2(1)(a) and (b), as regards unmanned aircraft and their engines, propellers, components and equipment for remote control thereof

ANNEX II

List of offences referred to in Article 5, paragraph 1, first subparagraph, letter h), point iii)

Offences referred to in Article 5, paragraph 1, first subparagraph, letter h), point iii):

— terrorism,

— human trafficking,

— sexual exploitation of minors and child pornography,

— illicit trafficking in narcotics or psychotropic substances,

— illicit trafficking in arms, ammunition and explosives,

— voluntary manslaughter, assault with serious injury,

— illicit trafficking in human organs or tissues,

— illicit trafficking in nuclear or radioactive materials,

— kidnapping, unlawful detention or hostage-taking,

— crimes that fall under the jurisdiction of the International Criminal Court,

— hijacking of aircraft or ships,

— rape,

— crimes against the environment,

— organized or armed robbery,

— sabotage,

— participation in a criminal organisation involved in one or more of the crimes listed in this list.

ANNEX III

High-risk AI systems referred to in Article 6(2)

High-risk AI systems within the meaning of Article 6(2) are AI systems that fall into any of the following areas:

1. Biometrics, to the extent their use is permitted by applicable Union or national law:

   a) Remote biometric identification systems

   Excluded are AI systems intended to be used for biometric verification purposes whose sole purpose is to confirm that a specific natural person is the person they claim to be.

   b) AI systems intended to be used for biometric categorization based on sensitive or protected attributes or characteristics based on inference of such attributes or characteristics

   c) AI systems intended to be used for emotion recognition

2. Critical infrastructures: AI systems intended to be used as security components in the management and operation of critical digital infrastructures, road traffic or the supply of water, gas, heating or electricity

3. Education and vocational training:

   a) AI systems intended to be used to determine the access or admission of natural persons to educational and vocational training establishments at all levels or to distribute natural persons between such establishments

   b) AI systems intended to be used to assess learning outcomes, including when such outcomes are used to guide the learning process of natural persons in educational and vocational training establishments at all levels

   c) AI systems intended to be used to assess the appropriate level of education that a person will receive or be able to access, in the context of educational and vocational training centres or within these at all levels

   d) AI systems intended to be used for monitoring and detecting prohibited behaviour by students during examinations in the context of educational and vocational training institutions or within these at all levels

4. Employment, employee management and access to self-employment:

   a) AI systems intended to be used for the recruitment or selection of natural persons, in particular for publishing targeted job advertisements, analysing and filtering job applications and evaluating candidates

   b) AI systems intended to be used to make decisions that affect the conditions of employment relationships or the promotion or termination of contractual employment relationships, for the assignment of tasks based on individual behavior or personal traits or characteristics or to monitor and evaluate the performance and behavior of individuals within the framework of such relationships.

5. Access to and enjoyment of essential private services and essential public services and benefits:

   (a) AI systems intended to be used by or on behalf of public authorities to assess the eligibility of natural persons for essential public assistance services and benefits, including healthcare services, and to grant, reduce, withdraw or claim their repayment;

   b) AI systems intended to be used to assess the creditworthiness of natural persons or establish their credit rating, except for AI systems used for the purpose of detecting financial fraud.

   c) AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance

(d) AI systems intended to be used for the assessment and classification of emergency calls made by natural persons or for the dispatch or prioritisation of dispatch of first responders in emergency situations, for example police, fire and medical services, and in patient triage systems in the context of emergency healthcare

6. Ensuring compliance with the law, to the extent that its use is permitted by applicable Union or national law:

(a) AI systems intended for use by or on behalf of law enforcement authorities or by Union institutions, bodies, offices and agencies in support of or on behalf of law enforcement authorities to assess the risk of a natural person becoming a victim of criminal offences

(b) AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices and agencies in support of law enforcement authorities such as polygraphs or similar tools

(c) AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices and agencies in support of law enforcement authorities to assess the reliability of evidence during the investigation or prosecution of criminal offences

(d) AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices and agencies supporting law enforcement authorities to assess the risk that a natural person will commit a criminal offence or reoffend, taking into account not only the profiling of natural persons referred to in point (4) of Article 3 of Directive (EU) 2016/680 or to assess personality traits and characteristics or past criminal behaviour of natural persons or collectives;

(e) AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices and agencies in support of law enforcement authorities for profiling natural persons, as referred to in point (4) of Article 3 of Directive (EU) 2016/680, during the detection, investigation or prosecution of criminal offences

7. Migration, asylum and border control management, to the extent that their use is permitted by applicable Union or national law:

(a) AI systems intended for use by or on behalf of the competent public authorities or by the Union institutions, bodies, offices and agencies, such as polygraphs or similar tools

(b) AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices and agencies to assess a risk, such as a risk to security, health or irregular migration, posed by a natural person intending to enter or having entered the territory of a Member State

(c) AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices and agencies to assist the competent public authorities in examining applications for asylum, visas or residence permits and related claims with a view to determining whether the applicant natural persons meet the requirements for their application to be granted, including the related assessment of the reliability of the evidence;

(d) AI systems intended for use by or on behalf of competent public authorities or by Union institutions, bodies, offices and agencies in the context of migration, asylum or border control management, for the purpose of detecting, recognising or identifying natural persons, with the exception of the verification of travel documents

8. Administration of justice and democratic processes:

(a) AI systems intended to be used by or on behalf of a judicial authority to assist a judicial authority in the investigation and interpretation of facts and the law, as well as in ensuring compliance with the Law on a particular set of facts, or to be used in a similar way in alternative dispute resolution;

(b) AI systems intended to be used to influence the outcome of an election or referendum or the voting behaviour of natural persons exercising their right to vote in elections or referendums. AI systems whose output results are not directly exposed to natural persons are excluded, such as tools used to organise, optimise or structure political campaigns from an administrative or logistical point of view.

ANNEX IV

Technical documentation referred to in Article 11, paragraph 1

The technical documentation referred to in Article 11(1) shall include at least the following information, applicable to the relevant AI system:

1. An overview of the AI system including:

a) its intended purpose, the name of the vendor and the version of the system in such a way as to reflect its relationship to previous versions;

b) the manner in which the AI system interacts or can be used to interact withhardwareeithersoftware,also with other AI systems, which are not part of the AI system itself, where applicable;

c) the versions ofsoftwareeitherfirmwarerelevant and any requirements related to version updates;

(d) a description of all the ways in which the AI system is introduced into the market or put into service, such as software packages integrated into the AI system;hardware,downloads or API;

e) the description of thehardwareon which the AI system is intended to run;

f) in the case where the AI system is a component of a product, photographs or illustrations of the external features, marking and internal configuration of said product;

g) a basic description of the user interface provided to the deployer;

h) instructions for use for the deployer and a basic description of the user interface provided to the deployer, where applicable.

2. A detailed description of the elements of the AI system and its development process, including:

(a) the methods and measures adopted for the development of the AI system, including, where applicable, the use of pre-trained systems or tools provided by third parties and the manner in which they have been used, integrated or modified by the provider;

(b) the design specifications of the system, namely the overall logic of the AI system and the algorithms; the key design decisions, including the logic and assumptions made, including with respect to the persons or groups of persons in relation to whom the system is intended to be used; the key classification decisions; what the system is designed to optimise and the relevance of the various parameters; the description of the expected output results of the system and the quality of those results; the decisions taken on any possible trade-offs with respect to the technical solutions adopted to meet the requirements set out in Chapter III, Section 2;

c) the system architecture, with an explanation of how the components of the system work together. softwareare used or enrich each other and how they are integrated into overall processing; the computing resources used to develop, train, test and validate the AI system;

(d) where applicable, data requirements, in the form of data sheets describing training methodologies and techniques, as well as the training data sets used, including an overview of such data sets and information about their provenance, scope and main characteristics; how the data were obtained and selected; labelling procedures (e.g. for supervised learning) and data cleaning methodologies (e.g. anomaly detection);

(e) an assessment of the necessary human oversight measures in accordance with Article 14, including an assessment of the technical measures necessary to facilitate the interpretation of the output results of AI systems by those responsible for deploying them, in accordance with point (d) of Article 13(3);

(f) where applicable, a detailed description of the predetermined changes to the AI system and its operation, together with all relevant information concerning the technical solutions adopted with the aim of ensuring the continued conformity of the AI system with the relevant requirements set out in Chapter III, Section 2;

(g) the validation and test procedures used, including information about the validation and test data used and their main characteristics; the parameters used to measure accuracy, robustness and compliance with other relevant requirements set out in Chapter III, Section 2, as well as any potentially discriminatory effects; the test log files and all test reports dated and signed by the responsible persons, also with regard to the default changes referred to in point (f);

h) the cybersecurity measures adopted.

3. Detailed information about the monitoring, operation and control of the AI system, in particular with regard to its operating capabilities and limitations, including the levels of accuracy for the specific persons or groups of persons in relation to whom the system is intended to be used and the overall level of accuracy expected in relation to its intended purpose; the foreseeable unintended outcomes and sources of risk to health and safety, fundamental rights and discrimination, in view of the intended purpose of the AI system; the necessary human oversight measures in accordance with Article 14, including technical measures put in place to facilitate the interpretation of the output results of AI systems by those responsible for deploying them; the specifications of the input data, as applicable.

4. A description of the suitability of the performance parameters for the specific AI system. A

5. detailed description of the risk management system in accordance with Article 9.

6. A description of the relevant changes made by the vendor to the system throughout its lifecycle.

7. A list of harmonized standards, applied in whole or in part, whose references have been published in the Official Journal of the European Union;Where harmonised standards have not been applied, a detailed description of the solutions adopted to meet the requirements set out in Chapter III, Section 2, including a list of other relevant standards and technical specifications that have been applied.

8. A copy of the EU declaration of conformity in accordance with Article 47.

9. A detailed description of the system established to assess the performance of the AI system in the post-market phase, in accordance with Article 72, including the post-market surveillance plan referred to in Article 72(3).

ANNEX V

EU Declaration of Conformity

The EU declaration of conformity referred to in Article 47 shall contain all of the following information:

1. The name and type of the AI   system, and any additional unambiguous references that allow the identification and traceability of the AI   system.
2. The name and address of the supplier or, where applicable, of its authorized representative.
3. The statement that the EU declaration of conformity pursuant to Article 47 is issued under the sole responsibility of the supplier.
4. The declaration that the AI   system complies with this Regulation and, where applicable, with any other relevant provisions of Union law providing for the issue of the EU declaration in accordance with Article 47.
5. Where an AI system involves the processing of personal data, a statement that the AI   system complies with Regulation (EU) 2016/679, Regulation (EU) 2018/1725 and Directive (EU) 2016/680.
6. References to any relevant harmonised standards that have been applied or to any other common specification to which conformity is declared.
7. Where applicable, the name and identification number of the notified body, a description of the conformity assessment procedure followed and the identification of the certificate issued.
8. The place and date of issue of the declaration, the name and position of the person who signs it, the indication of the person in whose name or on whose behalf the declaration is signed and the signature.

ANNEX VI

Conformity assessment procedure based on internal control

1. The conformity assessment procedure based on internal control is the conformity assessment procedure based on points 2, 3 and 4.

2. The supplier verifies that the established quality management system complies with the requirements set out in Article 17.

3. The supplier examines the information in the technical documentation to assess the conformity of the AI system with the relevant essential requirements set out in Chapter III, Section 2.

4. The supplier shall also verify that the design and development process of the AI system and its post-market surveillance referred to in Article 72 are consistent with the technical documentation.

ANNEX VII

Conformity based on the evaluation of the quality management system and the evaluation of the technical documentation

1. Introduction

Conformity based on assessment of the quality management system and assessment of technical documentation is the conformity assessment procedure based on points 2 to 5.

2. General presentation

The approved quality management system relating to the design, development and testing of AI systems pursuant to Article 17 shall be examined in accordance with point 3 and shall be subject to surveillance in accordance with point 5. The technical documentation of the AI system shall be examined in accordance with point 4.

3. Quality management system

3.1. The supplier's request shall include:

(a) the name and address of the supplier and, if the request is submitted by the authorised representative, also his name and address;

b) the list of AI systems to which the same quality management system applies;

c) the technical documentation of each AI system to which the same quality management system is applied;

(d) documentation relating to the quality management system, which shall cover all aspects listed in Article 17;

e) a description of the procedures established to ensure that the quality management system remains adequate and effective;

(f) a written declaration that the same application has not been submitted to any other notified body.

3.2. The quality management system shall be assessed by the notified body to determine whether it complies with the requirements specified in Article 17.

The decision will be notified to the supplier or his authorized representative.

The notification shall include the conclusions of the assessment of the quality management system and a reasoned decision on the assessment.

3.3. The supplier shall continue to implement and maintain the approved quality management system so that it remains suitable and effective.

3.4. The supplier shall inform the notified body of any intended changes to the approved quality management system or to the list of AI systems to which it applies.

The notified body shall examine the proposed changes and decide whether the modified quality management system continues to meet the requirements referred to in point 3.2 or whether a new assessment is necessary.

The notified body shall notify the supplier of its decision. The notification shall include the conclusions of the examination of the changes and a reasoned decision on the assessment.

4. Control of technical documentation

4.1. In addition to the application referred to in point 3, the supplier shall submit an application to the notified body of its choice for the assessment of the technical documentation relating to the AI system which the supplier intends to place on the market or put into service and to which the quality management system referred to in point 3 applies.

4.2. The application shall include:

a) the name and address of the supplier;

b) a written declaration that the same application has not been submitted to any other notified body;

c) the technical documentation provided for in Annex IV.

4.3. The notified body shall examine the technical documentation. Where appropriate, and to the extent necessary for the performance of its tasks, the notified body shall be granted full access to the training, validation and test data sets used, including, where appropriate and subject to security safeguards, through API or other relevant technical tools and means that allow remote access.

4.4. When examining the technical documentation, the notified body may require the supplier to provide further evidence supporting documents or carry out additional tests to enable the conformity of the AI system with the requirements set out in Chapter III, Section 2 to be properly assessed. Where the notified body is not satisfied with the tests carried out by the supplier, it shall itself carry out appropriate tests directly, as appropriate.

4.5. The notified body shall also be granted access to the training model and the trained model of the AI system, with its corresponding parameters, in order, if necessary, once all other reasonable means of verifying compliance have been exhausted and have proven insufficient, and upon reasoned request, to assess the compliance of the high-risk AI system with the requirements set out in Chapter III, Section 2. Such access shall be subject to applicable Union law on the protection of intellectual property and trade secrets.

4.6. The supplier or his authorised representative shall be notified of the decision of the notified body. The notification shall include the conclusions of the assessment of the technical documentation and a reasoned decision on the assessment.

Where the AI system complies with the requirements set out in Chapter III, Section 2, the notified body shall issue a Union certificate of assessment of the technical documentation. That certificate shall indicate the name and address of the supplier, the conclusions of the examination, the conditions of validity (if applicable) and the data necessary to identify the AI system.

The certificate and its annexes shall contain all relevant information to enable the conformity of the AI system to be assessed and to enable control of the AI system while in use, where applicable.

Where the AI system does not comply with the requirements set out in Chapter III, Section 2, the notified body shall refuse to issue the Union certificate of assessment of the technical documentation and shall inform the applicant thereof, giving detailed reasons for its decision.

Where the AI system does not comply with the requirements relating to the data used for its training, a new training of the system shall be required before requesting a new conformity assessment. In this case, the reasoned decision on the assessment by the notified body refusing to issue the Union certificate for assessment of technical documentation shall contain specific considerations relating to the quality of the data used to train the AI system, in particular regarding the reasons for the non-compliance.

4.7. Any changes to the AI system that may affect its compliance with the requirements or its intended purpose shall be assessed by the notified body that issued the Union certificate for assessment of technical documentation. The supplier shall inform the notified body of its intention to introduce any of the above-mentioned changes or of its knowledge of such changes. The notified body shall assess the intended changes and decide whether they require a new conformity assessment in accordance with Article 43(4) or whether they may be subject to a supplement to the Union certificate for assessment of technical documentation. In the latter case, the notified body shall assess the changes, notify its decision to the supplier and, if it approves the changes, issue a supplement to the Union certificate for assessment of technical documentation.

5. Monitoring of the approved quality management system

5.1. The purpose of surveillance by the notified body referred to in point 3 is to ensure that the supplier duly complies with the conditions of the approved quality management system.

5.2. For the purposes of the assessment, the supplier shall grant the notified body access to the premises where the AI systems are being designed, developed or tested. In addition, the supplier shall provide the notified body with all necessary information.

5.3. The notified body shall carry out periodic audits to ensure that the supplier maintains and applies the quality management system and shall provide the notified body with an audit report. Within the framework of such audits, the notified body may carry out further tests on AI systems for which Union certificates for the assessment of technical documentation have been issued.

ANNEX VIII

Information to be submitted for registration in the high-risk AI systems registry in accordance with article 49

Section A — Information to be submitted by providers of high-risk AI systems in accordance with the Article 49, paragraph 1

For high-risk AI systems to be registered pursuant to Article 49(1), the following information shall be provided and duly updated:

1. The name, address and contact details of the supplier.

2. When another person submits the information on behalf of the supplier, the name, address and contact details of that person.

3. The name, address and contact details of the authorised representative, if applicable.

4. The commercial name of the AI system and any additional unambiguous reference that allows its identification and traceability.

5. The description of the intended purpose of the AI system and the components and functions supported by it.

6. A simple and concise description of the information the system uses (data, inputs) and its operating logic.

7. The status of the AI system (marketed or put into service, no longer marketed or in service, recovered).

8. The type, number and expiry date of the certificate issued by the notified body and the name or identification number of the notified body, where applicable.

9. A scanned copy of the certificate referred to in point 8, where applicable.

10. Any Member State in which the AI system has been placed on the market, put into service or made available on the market in the Union.

11. A copy of the EU declaration of conformity referred to in Article 47.

12. Electronic instructions for use. This information shall not be provided for high-risk AI systems in the areas of law enforcement or migration, asylum and border control management.
referred to in Annex III, points 1, 6 and 7.

13. A URL for additional information (optional).

Section B — Information to be submitted by providers of high-risk AI systems in accordance with the Article 49, paragraph 2

With regard to AI systems to be registered pursuant to Article 49(2), the following information shall be provided and duly updated:

1. The name, address and contact details of the supplier.

2. When another person submits the information on behalf of the supplier, the name, address and contact details of that person.

3. The name, address and contact details of the authorised representative, if applicable.

4. The commercial name of the AI system and any additional unambiguous reference that allows its identification and traceability.

5. The description of the intended purpose of the AI system.

6. The condition or conditions referred to in Article 6(3) under which the AI system is considered not to be high risk.

7. A brief summary of the reasons why the AI system is considered not to be high risk in application of the procedure laid down in Article 6(3).

8. The status of the AI system (marketed or put into service, no longer marketed or in service, recovered).

9. Any Member State in which the AI system has been placed on the market, put into service or marketed within the Union.

Section C — Information to be submitted by those responsible for deploying high-risk AI systems
in accordance with Article 49, paragraph 3

For high-risk AI systems to be registered pursuant to Article 49(3), the following information shall be provided and duly updated:

1. The name, address and contact details of the person responsible for the deployment.

2. The name, address and contact details of the person submitting the information on behalf of the person responsible for deployment.

3. The URL of the AI system's entry into the EU database by its provider.

4. A summary of the findings of the fundamental rights impact assessment carried out in accordance with Article 27.

5. A summary of the data protection impact assessment carried out in accordance with Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, as specified in Article 26(8) of this Regulation, where applicable.

ANNEX IX

Information to be submitted for registration of high-risk AI systems listed in Annex III in relation to real-world compliance testing with article 60

With regard to real-life tests to be entered into the register pursuant to Article 60, the following information shall be provided and duly updated:

1. The unique identification number for the entire Union of the test under real conditions.
2. The name and contact details of the supplier or potential supplier and those responsible for deployment involved in the real-life test.
3. A brief description of the AI system, its intended purpose, and other information necessary to identify the system.
4. A summary of the main features of the real-world test plan. Information on the
5. suspension or termination of the real-world test.

ANNEX X

Legislative acts of the Union relating to large-scale information technology systems in the area of freedom, security and justice

1. Schengen Information System

(a) Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for returning illegally staying third-country nationals (OJ L 312, 7.12.2018, p. 1).

b) Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending the Convention implementing the Schengen Agreement and amending and repealing Regulation (EC) No 1861/2009.either1987/2006 (OJ L 312 of 7.12.2018, p. 14).

(c) Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1862/2009 of the European Parliament and of the Council.either1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56).

2. Visa Information System

a) Regulation (EU) 2021/1133 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EU) No.either603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 and (EU) 2019/818 as regards establishing the conditions for access to other EU information systems for the purposes of the Visa Information System (OJ L 248, 13.7.2021, p. 1).

b) Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 1134/2009 and (EC) No 1134/2009 and (EC) No 1134/2009.either767/2008, (EC) n.either810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, in order to reform the Visa Information System (OJ L 248, 13.7.2021, p. 11).

3. Eurodac

(a) Regulation (EU) 2024/1358 of the European Parliament and of the Council of 14 May 2024 on the establishment of 'Eurodac' for the comparison of biometric data for the effective application of Regulations (EU) 2024/1315 and (EU) 2024/1350 of the European Parliament and of the Council and Council Directive 2001/55/EC and the identification of illegally staying third-country nationals and stateless persons and on requests by Member States' law enforcement authorities and Europol for the purposes of law enforcement, amending Regulations (EU) 2018/1240 and (EU) 2019/818 of the European Parliament and of the Council and repealing Regulation (EU) No 1389/2008.either603/2013 of the European Parliament and of the Council (OJ L, 2024/1358, 22.5.2024, ELI: http://data.europa.eu/eli/reg/ 2024/1358/oj).

4. Input and Output System

(a) Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) for recording entry and exit data and refusal of entry data concerning third-country nationals crossing the external borders of the Member States, determining the conditions of access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 1789/2008 and (EC) No 1789/2008.either767/2008 and (EU) n.either1077/2011 (OJ L 327 of 9.12.2017, p. 20).

5. European Travel Information and Authorisation System

(a) Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No.either1077/2011, (EU) n.either515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).

b) Regulation (EU) 2018/1241 of the European Parliament and of the Council of 12 September 2018 amending Regulation (EU) 2016/794 for the purpose of establishing the European Travel Information and Authorisation System (ETIAS) (OJ L 236, 19.9.2018, p. 72).

6. European Criminal Records Information System in relation to third-country nationals and stateless persons

Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information concerning third-country nationals and stateless persons (ECRIS-TCN) to complement the European Criminal Records Information System, and amending Regulation (EU) 2018/1726 (OJ L 135, 22.5.2019, p. 1).

7. Interoperability

(a) Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 1189/2008 and (EC) No 1189/2008 and (EC) No 1189/2008.either767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).

(b) Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (OJ L 135, 22.5.2019, p. 85).

ANNEX XI

Technical documentation referred to in Article 53, paragraph 1, letter a) — technical documentation for general purpose AI model providers

Section 1

Information to be submitted by general-purpose AI model providers

The technical documentation referred to in Article 53, paragraph 1, letter a) shall include at least the following information depending on the size and risk profile of the model:

1. An overview of the general-purpose AI model including:

   a) the tasks that the model is to perform and the type and nature of the AI systems into which it can be integrated;

   b) the applicable acceptable use policies;

   c) the release date and distribution methods;

   d) the architecture and the number of parameters;

   e) the modality (e.g. text, image) and format of inputs and outputs;

   f) the license.

2. A detailed description of the elements of the model referred to in point 1 and relevant information on the development process, including the following elements:

   a) the technical means (e.g. instructions for use, infrastructure, tools) necessary to integrate the general-purpose AI model into AI systems;

   (b) the design specifications of the model and the training process, including training methods and techniques, key design decisions including rationale and assumptions made, what the model is designed to optimise and the appropriateness of the various parameters, as applicable;

   (c) information on the data used for training, testing and validation, where applicable, including the type and provenance of data and data management methods (e.g. cleaning, filtering, etc.), the number of data points, their scope and main characteristics; how the data were obtained and selected, as well as any other measures to detect unsuitable data sources and methods to detect identifiable biases, where applicable;

   d) the computational resources used to train the model (e.g., number of floating point operations, training time, and other relevant details related to the model;

   e) the known or estimated energy consumption of the model.

   Regarding letter e), when the energy consumption of the model is unknown, an estimate of the energy consumption may be made from information relating to the computational resources used.

Section 2

Additional information to be submitted by providers of general-purpose AI models with systemic risk

1. A detailed description of the evaluation strategies, with the results of the evaluation, based on publicly available evaluation protocols and tools or other evaluation methods. The evaluation strategies will include the evaluation criteria, parameters and the method of detection of limitations.

2. Where applicable, a detailed description of the measures taken to perform internal or external adversarial testing (e.g. use of "red teams") and adaptations of models, including their alignment and tuning.

3. Where applicable, a detailed description of the system architecture, with an explanation of how the software components incorporate or enrich each other and how they are integrated into overall processing.

ANNEX XII

Transparency information referred to in Article 53(1)(b) — technical documentation from providers of general-purpose AI models to downstream providers

integrate the model into your AI system

The information referred to in Article 53(1)(b) shall include at least the following information: 1. A

general description of the general-purpose AI model, including:

a) the tasks that the model is to perform and the type and nature of the AI systems into which it can be integrated;

b) the applicable acceptable use policies;

c) the release date and distribution methods;

d) the way in which the model interacts or can be used to interact with thehardwareor software that is not part of the model itself, where applicable;

(e) the versions of the relevant software related to the use of the general-purpose AI model, where applicable;

f) the architecture and the number of parameters;

g) the modality (e.g. text, image) and format of inputs and outputs;

h) the model license.

2. A description of the elements of the model and its development process, including:

a) the technical means (e.g. instructions for use, infrastructure, tools) necessary to integrate the general-purpose AI model into AI systems;

b) the modality (e.g. text, image, etc.) and format of the inputs and outputs and their maximum size (e.g. context window length, etc.);

c) information on data used for training, testing and validation, where applicable, including the type and source of data and management methods.

ANNEX XIII

Criteria for the classification of general-purpose AI models with systemic risk to which they are subject Article 51 refers

In order to determine whether a general-purpose AI model has capabilities or effects equivalent to those referred to in Article 51(1)(a), the Commission shall take into account the following criteria:

a) the number of parameters of the model;

b) the quality or size of the data set, for example measured through cryptotokens;

c) the amount of computation used to train the model, measured in floating point operations or indicated by a combination of other variables, such as the estimated cost of training, the estimated time required, or the estimated energy consumption for training;

d) the input and output modalities of the model, such as text-to-text (large language models), text-to-image, multimodality, and cutting-edge thresholds to determine the high-impact capabilities of each modality, and the specific type of inputs and outputs (e.g., biological sequences);

and) the benchmarks and assessments of the model's capabilities, also taking into account the number of tasks without additional training, its adaptability to learn different new tasks, its level of autonomy and expandability, and the tools to which it has access;

F) if its implications for the internal market are significant due to its scope, which will be the case when it has been made available to at least 10 000 registered professional users established in the Union;

g) the number of registered end users.