Official Journal
of the European Union

EN
L series

2024/1689

12.7.2024

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

of 13 June 2024

laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

(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,

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

Having regard to the opinion of the European Economic and Social Committee ([1]),

Having regard to the opinion of the European Central Bank ([2]),

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

Acting in accordance with the ordinary legislative procedure ([4]),

Whereas:

(1) The purpose of this Regulation is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence systems (AI systems) in the Union, in accordance with Union values, to promote the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (the 'Charter'), including democracy, the rule of law and environmental protection, to protect against the harmful effects of AI systems in the Union, and to support innovation. This Regulation ensures the free movement, cross-border, of AI-based goods and services, thus

preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation.

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

(3)AI systems can be easily deployed in a large variety of sectors of the economy and many parts of society, including across borders, and can easily circulate throughout the Union. Certain Member States have already explored the adoption of national rules to ensure that AI is trustworthy and safe and is developed and used in accordance with fundamental rights obligations. Diverging national rules may lead to the fragmentation of the internal market and may decrease legal certainty for operators that develop, import or use AI systems. A consistent and high level of protection throughout the Union should therefore be ensured in order to achieve trustworthy AI, while divergences hampering the free circulation, innovation, deployment and the uptake of AI systems and related products and services within the internal market should be prevented by laying down uniform obligations for operators and guaranteeing the uniform protection of overriding reasons of public interest and of rights of persons throughout the internal market 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 on the protection of individuals with regard to the processing of personal data concerning restrictions of the use of AI systems for remote biometric identification for the purpose of law enforcement, of the use of AI systems for risk assessments of natural persons for the purpose of law enforcement and of the use of AI systems of biometric categorisation for the purpose of law enforcement, it is appropriate to base this Regulation, in so far as those specific rules are concerned, on Article 16 TFEU. In 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 fast evolving family of technologies that contributes to a wide array of economic, environmental and societal benefits across the entire spectrum of industries and social activities. By improving prediction, optimising operations and resource allocation, and personalising digital solutions available for individuals and organisations, the use of AI can provide key competitive advantages to undertakings and support socially and environmentally beneficial outcomes, for example in healthcare, agriculture, food safety, education and training, media, sports, culture, infrastructure management, energy, transport and logistics, public services, security, justice, resource and energy efficiency, environmental monitoring, the conservation and restoration of biodiversity and ecosystems and climate change mitigation and adaptation.

(5)At the same time, depending on the circumstances regarding its specific application, use, and level of technological development, AI may generate risks and cause harm to public interests and fundamental rights that are protected by Union law. Such harm might be material or immaterial, including physical, psychological, societal or economic harm.

(6) Given the major impact that AI can have on society and the need to build trust, it is vital for AI and its regulatory framework to be developed in accordance with Union values as enshrined in Article 2 of the Treaty on European Union (TEU), the fundamental rights and freedoms enshrined in the Treaties and, pursuant to Article 6 TEU, the Charter. As a prerequisite, AI should be a human-centric technology. It should serve as a tool for people, with the ultimate aim of increasing human well-being.

(7) In order to ensure a consistent and high level of protection of public interests as regards health, safety and fundamental rights, common rules for high-risk AI systems should be established. Those rules should be consistent with the Charter, non-discriminatory and in line with the Union's international trade commitments. They should also take into account the European Declaration on Digital Rights and Principles for the Digital Decade and the Ethics guidelines for trustworthy AI of the High-Level Expert Group on Artificial Intelligence (AI HLEG).

(8) A Union legal framework laying down harmonised rules on AI is therefore needed to foster the development, use and uptake of AI in the internal market that at the same time meets a high level of protection of public interests, such as health and safety and the protection of fundamental rights, including democracy, the rule of law and environmental protection as recognised and protected by Union law. To achieve that objective, rules regulating the placing on the market, the putting into service and the use of certain AI systems should be laid down, thus ensuring the smooth functioning of the internal market and allowing those systems to benefit from the principle of free movement of goods and services. Those rules should be clear and robust in protecting fundamental rights, supportive of new innovative solutions, enabling a European ecosystem of public and private actors creating AI systems in line with Union values and unlocking the potential of the digital transformation across all regions of the Union. By laying down those rules as well as measures in support of innovation with a particular focus on small and medium enterprises (SMEs), including startups, this Regulation supports the objective of promoting the European human-centric approach to AI and being a global leader in the development of secure, trustworthy and ethical AI as stated by the European Council [5], and it ensures the protection of ethical principles, as specifically requested by the European Parliament [6].

(9) Harmonised rules applicable to the placing on the market, the putting into service and the use of high-risk AI systems should be laid down consistently with Regulation (EC) No 765/2008 of the European Parliament and of the Council [7], Decision No 768/2008/EC of the European Parliament and of the Council [8] and Regulation (EU) 2019/1020 of the European Parliament and of the Council [9] (New Legislative Framework). The harmonised rules laid down in this Regulation should apply across 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, and protection of workers, and product safety, to which this Regulation is complementary. As a consequence, all rights and remedies provided for by such Union law to consumers, and other persons on whom AI systems may have

a negative impact, including as regards the compensation of possible damages pursuant to Council Directive 85/374/EEC ([10]) remain unaffected and fully applicable. Furthermore, in the context of employment and protection of workers, this Regulation should therefore not affect Union law on social policy and national labour law, in compliance with Union law, concerning employment and working conditions, including health and safety at work and the relationship between employers and workers. This Regulation should also not affect the exercise of fundamental rights as recognised in the Member States and at Union level, including the right or freedom to strike or to take other action covered by the specific industrial relations systems in Member States as well as the right to negotiate, to conclude and enforce collective agreements or to take collective action in accordance with national law. This Regulation should not affect the provisions aiming to improve working conditions in platform work laid down in a Directive of the European Parliament and of the Council on improving working conditions in platform work. Moreover, this Regulation aims to strengthen the effectiveness of such existing rights and remedies by establishing specific requirements and obligations, including in respect of the transparency, technical documentation and record-keeping of AI systems. Furthermore, the obligations placed on various operators involved in the AI value chain under this Regulation should apply without prejudice to national law, in compliance with Union law, having 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. For example, national labour law and law on the protection of minors, namely persons below the age of 18, taking into account the UNCRC General Comment No 25 (2021) on children's rights in relation to the digital environment, insofar as they are not specific to AI systems and pursue other legitimate public interest objectives, should not be affected by this Regulation.

(10) The fundamental right to the protection of personal data is safeguarded in particular by 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]). Directive 2002/58/EC of the European Parliament and of the Council ([14]) additionally protects private life and the confidentiality of communications, including by way of providing conditions for any storing of personal and non-personal data in, and access from, terminal equipment. Those Union legal acts provide the basis for sustainable and responsible data processing, including where data sets include a mix of personal and non-personal data. This Regulation does not seek to affect the application of existing Union law governing the processing of personal data, including the tasks and powers of the independent supervisory authorities competent to monitor compliance with those instruments. It also does not affect the obligations of providers and deployers of AI systems in their role as data controllers or processors stemming from Union or national law on the protection of personal data in so far as the design, the development or the use of AI systems involves the processing of personal data. It is also appropriate to clarify that data subjects continue to enjoy all the rights and guarantees awarded to them by such Union law, including the rights related to solely automated individual decision-making, including profiling. Harmonised rules for the placing

on the market, the putting into service and the use of AI systems established under this Regulation should facilitate the effective implementation and enable the exercise of the data subjects' rights and other remedies guaranteed under Union law on the protection of personal data and of other fundamental rights.

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

(12) The notion of 'AI system' in this Regulation should be clearly defined and should be closely aligned with the work of international organisations working on AI to ensure legal certainty, facilitate international convergence and wide acceptance, while providing the flexibility to accommodate the rapid technological developments in this field. Moreover, the definition should be based on key characteristics of AI systems that distinguish it from simpler traditional software systems or programming approaches and should not cover systems that are based on the rules defined solely by natural persons to automatically execute operations. A key characteristic of AI systems is their capability to infer. This capability to infer refers to the process of obtaining the outputs, such as predictions, content, recommendations, or decisions, which can influence physical and virtual environments, and to a capability of AI systems to derive models or algorithms, or both, from inputs or data. The techniques that enable inference while building an AI system include machine learning approaches that learn from data how to achieve certain objectives, and logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved. The capacity of an AI system to infer transcends basic data processing by enabling learning, reasoning or modelling. The term 'machine-based' refers to the fact that AI systems run on machines. The reference to explicit or implicit objectives underscores that AI systems can operate according to explicit defined objectives or to 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 to be the contexts in which the AI systems operate, whereas outputs generated by the AI system reflect different functions performed by AI systems and include predictions, content, recommendations or decisions. AI systems are designed to operate with varying levels of autonomy, meaning that they have some degree of independence of actions from human involvement and of capabilities to operate without human intervention. The adaptiveness that an AI system could exhibit after deployment, refers to self-learning capabilities, allowing the system to change while in use. AI systems can be used on a stand-alone basis or as a component of a product, irrespective of whether the system is physically integrated into the product (embedded) or serves the functionality of the product without being integrated therein (non-embedded).

(13) The notion of 'deployer' referred to in this Regulation should be interpreted as any natural or legal person, including a public authority, agency or other body, using an AI system under its authority, except where the AI system is used in the course of a personal non-professional

activity. Depending on the type of AI system, the use of the system may affect persons other than the deployer.

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

(15)The notion of 'biometric identification' referred to in this Regulation should be defined as the automated recognition of physical, physiological and behavioural human features such as the face, eye movement, body shape, voice, prosody, gait, posture, heart rate, blood pressure, odour, keystrokes characteristics, for the purpose of establishing an individual's identity by comparing biometric data of that individual to stored biometric data of individuals in a reference database, irrespective of whether the individual has given its consent or not. This excludes AI systems intended to be used for biometric verification, which includes authentication, whose sole purpose is to confirm that a specific natural person is the person he or she claims to be and to confirm the identity of a natural person for the sole purpose of having access to a service, unlocking a device or having security access to premises.

(16)The notion of 'biometric categorisation' referred to in this Regulation should be defined as assigning natural persons to specific categories on the basis of their biometric data. Such specific categories can 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 that are a purely ancillary feature intrinsically linked to another commercial service, meaning that the feature cannot, for objective technical reasons, be used without the principal service, and the integration of that feature or functionality is not a means to circumvent the applicability of the rules of this Regulation. For example, filters categorising facial or body features used on online marketplaces could constitute such an ancillary feature as they can be used only in relation to the principal service which consists in selling a product by allowing the consumer to preview the display of the product on him or herself and help the consumer to make a purchase decision. Filters used on online social network services which categorise facial or body features to allow users to add or modify pictures or videos could also be considered to be ancillary feature as such filter cannot be used without the principal service of the social network services consisting in the sharing of content online.

(17)The notion of 'remote biometric identification system' referred to in this Regulation should be defined functionally, as an AI system intended for the identification of natural persons without their active involvement, typically at a distance, through the comparison of a person's biometric data with the biometric data contained in a reference database, irrespectively of the particular technology, processes or types of biometric data used. Such remote biometric identification systems are typically used to perceive multiple persons or their behaviour

simultaneously in order to facilitate significantly the identification of natural persons without their active involvement. This excludes AI systems intended to be used 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 and to confirm the identity of a natural person for the sole purpose of having access to a service, unlocking a device or having security access to premises. That exclusion is justified by the fact that such systems are likely to have a minor impact on fundamental rights of natural persons compared to the remote biometric identification systems which may be used for the processing of the biometric data of a large number of persons without their active involvement. In the case of 'real-time' systems, the capturing of the biometric data, the comparison and the identification occur all instantaneously, near-instantaneously or in any event without a significant delay. In this regard, there should be no scope for circumventing the rules of this Regulation on the 'real-time' use of the AI systems concerned by providing for minor delays. 'Real-time' systems involve the use of 'live' or 'near-live' material, such as video footage, generated by a camera or other device with similar functionality. In the case of 'post' systems, in contrast, the biometric data has already been captured and the comparison and identification occur only after a significant delay. This involves material, such as pictures or video footage generated by closed circuit television cameras or private devices, which has been generated before the use of the system in respect of the natural persons concerned.

(18) The notion of 'emotion recognition system' referred to in this Regulation should be defined as an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data. The notion refers to emotions or intentions such as happiness, sadness, anger, surprise, disgust, embarrassment, excitement, shame, contempt, satisfaction and amusement. It does not include physical states, such as pain or fatigue, including, for example, systems used in detecting the state of fatigue of professional pilots or drivers for the purpose of preventing accidents. This does also not include the mere detection of readily apparent expressions, gestures or movements, unless they are used for identifying or inferring emotions. Those expressions can be basic facial expressions, such as a frown or a smile, or gestures such as the movement of hands, arms or head, or characteristics of a person's voice, such as a raised voice or whispering.

(19) For the purposes of this Regulation the notion of 'publicly accessible space' should be understood as referring to any physical space that is accessible to an undetermined number of natural persons, and irrespective of whether the space in question is privately or publicly owned, irrespective of the activity for which the space may be used, such as for commerce, for example, shops, restaurants, cafés; for services, for example, banks, professional activities, hospitality; for sport, for example, swimming pools, gyms, stadiums; for transport, for example, bus, metro and railway stations, airports, means of transport; for entertainment, for example, cinemas, theatres, museums, concert and conference halls; or for leisure or otherwise, for example, public roads and squares, parks, forests, playgrounds. A space should also be classified as being publicly accessible if, regardless of potential capacity or security

restrictions, access is subject to certain predetermined conditions which can be fulfilled by an undetermined number of persons, such as the purchase of a ticket or title of transport, prior registration or having a certain age. In contrast, a space should not be considered to be publicly accessible if access is limited to specific and defined natural persons through either Union or national law directly related to public safety or security or through the clear manifestation of will by the person having the relevant authority over the space. The factual possibility of access alone, such as an unlocked door or an open gate in a fence, does not imply that the space is publicly accessible in the presence of indications or circumstances suggesting the contrary, such as. signs prohibiting or restricting access. Company and factory premises, as well as offices and workplaces that are intended to be accessed only by relevant employees and service providers, are spaces that are not publicly accessible. Publicly accessible spaces should not include prisons or border control. Some other spaces may comprise both publicly accessible and non-publicly accessible spaces, such as the hallway of a private residential building necessary to access a doctor's office or an airport. Online spaces are not covered, as they are not physical spaces. Whether a given space is accessible to the public should however be determined on a case-by-case basis, having regard to the specificities of the individual situation at hand.

(20) In order to obtain the greatest benefits from AI systems while protecting fundamental rights, health and safety and to enable democratic control, AI literacy should equip providers, deployers and affected persons with the necessary notions to make informed decisions regarding AI systems. Those notions may vary with regard to the relevant context and can include understanding the correct application of technical elements during the AI system's development phase, the measures to be applied during its use, the suitable ways in which to interpret the AI system's output, and, in the case of affected persons, the knowledge necessary to understand how decisions taken with the assistance of AI will have an impact on them. In the context of the application this Regulation, AI literacy should provide all relevant actors in the AI value chain with the insights required to ensure the appropriate compliance and its correct enforcement. Furthermore, the wide implementation of AI literacy measures and the introduction of appropriate follow-up actions could contribute to improving working conditions and ultimately sustain the consolidation, and innovation path of trustworthy AI in the Union. The European Artificial Intelligence Board (the 'Board') should support the Commission, to promote 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 the relevant stakeholders, the Commission and the Member States should facilitate the drawing up of voluntary codes of conduct to advance AI literacy among persons dealing with the development, operation and use of AI.

(21) In order to ensure a level playing field and an effective protection of rights and freedoms of individuals across the Union, the rules established by this Regulation should apply to providers of AI systems in a non-discriminatory manner, irrespective of whether they are established

within the Union or in a third country, and to deployers of AI systems established within the Union.

(22) In light of their digital nature, certain AI systems should fall within the scope of this Regulation even when 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 contracts certain services to an operator established in a third country in relation to an activity to be performed by an AI system that would qualify as high-risk. In those circumstances, the AI system used in a third country by the operator could process data lawfully collected in and transferred from the Union, and provide to the contracting operator in the Union the output of that AI system resulting from that processing, without that AI system being placed on the market, put into service or used in the Union. To prevent the circumvention of this Regulation and to ensure an effective protection of natural persons located in the Union, this Regulation should also apply to providers and deployers of AI systems that are established in a third country, to the extent the output produced by those systems is intended to be used in the Union. Nonetheless, to take into account existing arrangements and special needs for future cooperation with foreign partners with whom information and evidence is exchanged, this Regulation should not apply to public authorities of a third country and international organisations when acting in the framework of cooperation or international agreements concluded at Union or national level for law enforcement and judicial cooperation with the Union or the Member States, provided that the relevant third country or international organisation provides adequate safeguards with respect to the protection of fundamental rights and freedoms of individuals. Where relevant, this may cover activities of entities entrusted by the third countries to carry out specific tasks in support of such law enforcement and judicial cooperation. Such framework for cooperation or agreements have been established bilaterally between Member States and third countries or between the European Union, Europol and other Union agencies and third countries and international organisations. The authorities competent for supervision of the law enforcement and judicial authorities under this Regulation should assess whether those frameworks for cooperation or international agreements include adequate safeguards with respect to the protection of fundamental rights and freedoms of individuals. Recipient national authorities and Union institutions, bodies, offices and agencies making use of such outputs in the Union remain accountable to ensure their use complies with Union law. When those international agreements are revised or new ones are concluded in the future, the contracting parties should make utmost efforts to align those agreements with the requirements of this Regulation.

(23) This Regulation should also apply to Union institutions, bodies, offices and agencies when acting as a provider or deployer of an AI system.

(24) If, and insofar as, AI systems are placed on the market, put into service, or used with or without modification of such systems for military, defence or national security purposes, those should be excluded from the scope of this Regulation regardless of which type of entity is carrying out those activities, such as whether it is a public or 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' and the common Union defence policy covered by Chapter 2 of Title V TEU that are subject to public international law, which is therefore the more 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 sole responsibility of Member States in accordance with Article 4(2) TEU and by the specific nature and operational needs of national security activities and specific national rules applicable to those activities. Nonetheless, if an AI system developed, placed on the market, put into service or used for military, defence or national security purposes is used outside those temporarily or permanently for other purposes, for example, civilian or humanitarian purposes, law enforcement or public security purposes, such a system would fall within the scope of this Regulation. In that case, the entity using the AI system for other than military, defence or national security purposes should ensure the compliance of the AI system with this Regulation, unless the system is already compliant with this Regulation. AI systems placed on the market or put into service for an excluded purpose, namely military, defence or national security, and one or more non-excluded purposes, such as civilian purposes or law enforcement, fall within the scope of this Regulation and providers of those systems should ensure compliance with this Regulation. In those cases, the fact that an AI system may fall within the scope of this Regulation should not affect the possibility of entities carrying out national security, defence and military activities, regardless of the type of entity carrying out those activities, to use AI systems for national security, military and defence purposes, the use of which is excluded from the scope of this Regulation. An AI system placed on the market for civilian or law enforcement purposes which is used with or without modification 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, should respect freedom of science, and should not undermine research and development activity. It is therefore necessary to exclude from its scope AI systems and models specifically developed and put into service for the sole purpose of scientific research and development. Moreover, it is necessary to ensure that this Regulation does not otherwise affect scientific research and development activity on AI systems or models prior to being placed on the market or put into service. As regards product-oriented research, testing and development activity regarding AI systems or models, the provisions of this Regulation should also not apply prior to those systems and models being put into service or placed on the market. That exclusion is without prejudice to the obligation to comply with this Regulation where an AI system falling into the scope of this Regulation is placed on the market or put into service as a result of such research and development activity and to the application of provisions on AI regulatory sandboxes and testing in real world conditions. Furthermore, without prejudice to the exclusion of AI systems specifically developed and put into service for the sole purpose of scientific research and development, any other AI system that may be used for the conduct of 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 should be conducted in accordance with applicable Union law.

(26) In order to introduce a proportionate and effective set of binding rules for AI systems, a clearly defined risk-based approach should be followed. That approach should tailor the type and content of such rules to the intensity and scope of the risks that AI systems can generate. It is therefore necessary to prohibit certain unacceptable AI practices, to lay down requirements for high-risk AI systems and obligations for the relevant operators, and to lay down transparency obligations for certain AI systems.

(27) While the risk-based approach is the basis for a proportionate and effective set of binding rules, it is important to recall the 2019 Ethics guidelines for trustworthy AI developed by the independent AI HLEG appointed by the Commission. In those guidelines, the AI HLEG developed seven non-binding ethical principles for AI which are intended to help ensure that AI is trustworthy and ethically sound. The seven principles include human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental well-being and accountability. Without prejudice to the legally binding requirements of this Regulation and any other applicable Union law, those guidelines contribute to the design of coherent, trustworthy and human-centric AI, in line with the Charter and with the values on which the Union is founded. According to the guidelines of the AI HLEG, human agency and oversight means that AI systems are developed and used as a tool that serves people, respects human dignity and personal autonomy, and that is functioning in a way that can be appropriately controlled and overseen by humans. Technical robustness and safety means that AI systems are developed and used in a way that allows robustness in the case of problems and resilience against attempts to alter the use or performance of the AI system so as to allow unlawful use by third parties, and minimise unintended harm. Privacy and data governance means that AI systems are developed and used in accordance with privacy and data protection rules, while processing data that meets high standards in terms of quality and integrity. Transparency means that AI systems are developed and used in a way that allows appropriate traceability and explainability, while making humans aware that they communicate or interact with an AI system, as well as duly informing deployers of the capabilities and limitations of that AI system and affected persons 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 impacts and unfair biases that are 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 in a way to benefit all human beings, while monitoring and assessing the long-term impacts on the individual, society and democracy. The application of those principles should be translated, when possible, in the design and use of AI models. They should in any case serve as a basis for the drafting of codes of conduct under

this Regulation. All stakeholders, including industry, academia, civil society and standardisation organisations, are encouraged to take into account, as appropriate, the ethical principles for the development of voluntary best practices and standards.

(28) Aside from the many beneficial uses of AI, it can also be misused and provide novel and powerful tools for manipulative, exploitative and social control practices. Such practices are particularly harmful and abusive and should be prohibited because they contradict Union values of respect for human dignity, freedom, equality, democracy and the rule of law and fundamental rights enshrined in the Charter, including the right to non-discrimination, to data protection and to privacy and the rights of the child.

(29) AI-enabled manipulative techniques can be used to persuade persons to engage in unwanted behaviours, or to deceive them by nudging them into decisions in a way that subverts and impairs their autonomy, decision-making and free choices. The placing on the market, the putting into service or the use of certain AI systems with the objective to or the effect of materially distorting human behaviour, whereby significant harms, in particular having sufficiently important adverse impacts on physical, psychological health or financial interests are likely to occur, are particularly dangerous and should therefore be prohibited. Such AI systems deploy subliminal components such as audio, image, video stimuli that persons cannot perceive, as those stimuli are beyond human perception, or other manipulative or deceptive techniques that subvert or impair person's autonomy, decision-making or free choice in ways that people are not consciously aware of those techniques or, where they are aware of them, can still be deceived or are not able to control or resist them. This could be facilitated, for example, by machine-brain interfaces or virtual reality as they allow for a higher degree of control of what stimuli are presented to persons, insofar as they may materially distort their behaviour in a significantly harmful manner. In addition, AI systems may also otherwise exploit the vulnerabilities of a person or a specific group of persons due to their age, disability within the meaning of Directive (EU) 2019/882 of the European Parliament and of the Council ([16]), or a specific social or economic situation that is likely to make those persons more vulnerable to exploitation such as persons living in extreme poverty, ethnic or religious minorities. Such AI systems can be placed on the market, put into service or used with the objective to or the effect of materially distorting the behaviour of a person and in a manner that causes or is reasonably likely to cause significant harm to that or another person or groups of persons, including harms that may be accumulated over time and should therefore be prohibited. It may not be possible to assume that there is an intention to distort behaviour where the distortion results from factors external to the AI system which are outside the control of the provider or the deployer, namely factors that may not be reasonably foreseeable and therefore not possible for the provider or the deployer of the AI system to mitigate. In any case, it is not necessary for the provider or the deployer to have the intention to cause significant harm, provided that such harm results from the manipulative or exploitative AI-enabled practices. The prohibitions for such AI practices are complementary to the provisions contained in Directive 2005/29/EC of the European Parliament and of the Council ([17]), in

particular unfair commercial practices leading to economic or financial harms to consumers are prohibited under all circumstances, irrespective of whether they are put in place through AI systems or otherwise. The prohibitions of manipulative and exploitative practices in this Regulation should not affect lawful practices in the context of medical treatment such as psychological treatment of a mental disease or physical rehabilitation, when those practices are carried out in accordance with the applicable law and medical standards, for example explicit consent of the individuals or their legal representatives. In addition, common and legitimate commercial practices, for example in the field of advertising, that comply with the applicable law should not, in themselves, be regarded as constituting harmful manipulative AI-enabled practices.

(30) Biometric categorisation systems that are based on natural persons' biometric data, such as an individual person's face or fingerprint, to deduce or infer an individuals' political opinions, trade union membership, religious or philosophical beliefs, race, sex life or sexual orientation should be prohibited. That prohibition should not cover the lawful labelling, filtering or categorisation of biometric data sets acquired in line with Union or national law according to biometric data, such as the sorting of images according to hair colour or eye colour, which can for example be used in the area of law enforcement.

(31) AI systems providing social scoring of natural persons by public or private actors may lead to discriminatory outcomes and the exclusion of certain groups. They may violate the right to dignity and non-discrimination and the values of equality and justice. Such AI systems evaluate or classify natural persons or groups thereof on the basis of multiple data points related to their social behaviour in multiple contexts or known, inferred or predicted personal or personality characteristics over certain periods of time. The social score obtained from such AI systems may lead to the detrimental or unfavourable treatment of natural persons or whole groups thereof in social contexts, which are unrelated to the context in which the data was originally generated or collected or to a detrimental treatment that is disproportionate or unjustified to the gravity of their social behaviour. AI systems entailing such unacceptable scoring practices and leading to such detrimental or unfavourable outcomes should therefore be prohibited. That prohibition should not affect lawful evaluation practices of natural persons that are carried out for a specific purpose in accordance with Union and national law.

(32) The use of AI systems for 'real-time' remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement is particularly intrusive to the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights. Technical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to biased results and entail discriminatory effects. Such possible biased results and discriminatory effects are particularly relevant with regard to age, ethnicity, race, sex or disabilities. In addition, the immediacy of the impact and the limited opportunities for further checks or corrections in relation to the use of such systems operating in real-time carry

heightened risks for the rights and freedoms of the persons concerned in the context of, or impacted by, law enforcement activities.

(33) The use of those systems for the purpose of law enforcement should therefore be prohibited, except in exhaustively listed and narrowly defined situations, where the use is strictly necessary to achieve a substantial public interest, the importance of which outweighs the risks. Those situations involve the search for certain victims of crime including missing persons; certain threats to the life or to the physical safety of natural persons or of a terrorist attack; and the localisation or identification of perpetrators or suspects of the criminal offences listed in an annex to this Regulation, where those criminal offences are punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years and as they are defined in the law of that Member State. Such a threshold for the custodial sentence or detention order in accordance with national law contributes to ensuring that the offence should be serious enough to potentially justify the use of 'real-time' remote biometric identification systems. Moreover, the list of criminal offences provided in an annex to this Regulation is based on the 32 criminal offences listed in the Council Framework Decision 2002/584/JHA ([18]), taking into account that some of those offences are, in practice, likely to be more relevant than others, in that the recourse to 'real-time' remote biometric identification could, foreseeably, be necessary and proportionate to highly varying degrees for the practical pursuit of the localisation or identification of a perpetrator or suspect of the different criminal offences listed and having regard to the likely differences in the seriousness, probability and scale of the harm or possible negative consequences. An imminent threat to life or the physical safety of natural persons could also result from a serious disruption of critical infrastructure, as defined in Article 2, point (4) of Directive (EU) 2022/2557 of the European Parliament and of the Council ([19]), where the disruption or destruction of such critical infrastructure would result in an imminent threat to life or the physical safety of a person, including through serious harm to the provision of basic supplies to the population or to the exercise of the core function of the State. In addition, this Regulation should preserve the ability for 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 set out 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, either refuse to be identified or are unable to state or prove their identity, without being required by this Regulation to obtain prior authorisation. This could be, for example, a person involved in a crime, being unwilling, or unable due to an accident or a medical condition, to disclose their identity to law enforcement authorities.

(34) In order to ensure that those systems are used in a responsible and proportionate manner, it is also important to establish that, in each of those exhaustively listed and narrowly defined situations, certain elements should be taken into account, in particular as regards the nature of the situation giving rise to the request and the consequences of the use for the rights and

freedoms of all persons concerned and the safeguards and conditions provided for with the use. In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement should be deployed only to confirm the specifically targeted individual's identity and should be limited to what is strictly necessary concerning the period of time, as well as the geographic and personal scope, having regard in particular to the evidence or indications regarding the threats, the victims or perpetrator. The use of the real-time remote biometric identification system in publicly accessible spaces should be authorised only if the relevant law enforcement authority has completed a fundamental rights impact assessment and, unless provided otherwise in this Regulation, has registered the system in the database as set out in this Regulation. The reference database of persons should be appropriate for each use case in each of the situations mentioned above.

(35) Each use of a 'real-time' remote biometric identification system in publicly accessible spaces for the purpose of law enforcement should be subject to an express and specific authorisation by a judicial authority or by an independent administrative authority of a Member State whose decision is binding. Such authorisation should, in principle, be obtained prior to the use of the AI system with a view to identifying a person or persons. Exceptions to that rule should be allowed in duly justified situations on grounds of urgency, namely in situations where the need to use the systems concerned is such as to make it effectively and objectively impossible to obtain an authorisation before commencing the use of the AI system. In such situations of urgency, the use of the AI system should be restricted to the absolute minimum necessary and should be subject to appropriate safeguards and conditions, as determined in national law and specified in the context of each individual urgent use case by the law enforcement authority itself. In addition, the law enforcement authority should in such situations request such authorisation while providing the reasons for not having been able to request it earlier, without undue delay and at the latest within 24 hours. If such an authorisation is rejected, the use of real-time biometric identification systems linked to that authorisation should cease with immediate effect and all the data related to such use should be discarded and deleted. Such data includes input data directly acquired by an AI system in the course of the use of such system as well as the results and outputs of the use linked to that authorisation. It should not include input that is legally acquired in accordance with another Union or national law. In any case, no decision producing an adverse legal effect on a person should be taken based solely on the output 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 the national data protection authorities that have been notified should submit to the Commission an annual report on the use of real-time biometric identification systems.

(37) Furthermore, it is appropriate to provide, within the exhaustive framework set by this Regulation that such use in the territory of a Member State in accordance with this Regulation

should only be possible where and in as far as the Member State concerned has decided to expressly provide for the possibility to authorise such use in its detailed rules of national law. Consequently, Member States remain free under this Regulation not to provide for such a possibility at all or to only provide for such a possibility in respect of some of the objectives capable of justifying authorised use identified in this Regulation. Such national rules should be notified to the Commission within 30 days of their adoption.

(38) The use of AI systems for real-time remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement necessarily involves the processing of biometric data. The rules of this Regulation that prohibit, subject to certain exceptions, such use, which are based on Article 16 TFEU, should apply as *lex specialis* in respect of the rules on the processing of biometric data contained in Article 10 of Directive (EU) 2016/680, thus regulating such use and the processing of biometric data involved in an exhaustive manner. Therefore, such use and processing should be possible only in as far as it is compatible with the framework set by this Regulation, without there being scope, outside that framework, for the competent authorities, where they act for purpose of law enforcement, to use such systems and process such data in connection thereto on the grounds listed in Article 10 of Directive (EU) 2016/680. In that context, this Regulation is not intended to provide the legal basis for the processing of personal data under Article 8 of Directive (EU) 2016/680. However, the use of real-time remote biometric identification systems in publicly accessible spaces for purposes other than law enforcement, including by competent authorities, should not be covered by the specific framework regarding such use for the purpose of law enforcement set by this Regulation. Such use for purposes other than law enforcement should therefore not be subject to the requirement of an authorisation under this Regulation and the applicable detailed rules of national law that may give effect to that authorisation.

(39) Any processing of biometric data and other personal data involved in the use of AI systems for biometric identification, other than in connection to the use of real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement as regulated by this Regulation, should continue to comply with all requirements resulting from Article 10 of Directive (EU) 2016/680. For purposes other than law enforcement, Article 9(1) of Regulation (EU) 2016/679 and Article 10(1) of Regulation (EU) 2018/1725 prohibit the processing of biometric data subject to limited exceptions as provided 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 law enforcement has already been subject to prohibition decisions by national data protection authorities.

(40) In accordance with Article 6a of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the TEU and to the TFEU, Ireland is not bound by the rules laid down in Article 5(1), first subparagraph, point (g), to the extent it applies to the use of biometric categorisation systems for activities in the field of police cooperation and judicial cooperation in criminal matters, Article 5(1), first subparagraph, point (d), to the extent it applies to the use of AI systems covered by that

provision, Article 5(1), first subparagraph, point (h), Article 5(2) to (6) and Article 26(10) of this Regulation adopted on the basis of Article 16 TFEU which relate to the processing of personal data by the Member States when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU, where Ireland is not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16 TFEU.

(41) In accordance with Articles 2 and 2a of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not bound by rules laid down in Article 5(1), first subparagraph, point (g), to the extent it applies to the use of biometric categorisation systems for activities in the field of police cooperation and judicial cooperation in criminal matters, Article 5(1), first subparagraph, point (d), to the extent it applies to the use of AI systems covered by that provision, Article 5(1), first subparagraph, point (h), (2) to (6) and Article 26(10) of this Regulation adopted on the basis of Article 16 TFEU, or subject to their application, which relate to the processing of personal data by the Member States when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU.

(42) In line with the presumption of innocence, natural persons in the Union should always be judged on their actual behaviour. Natural persons should never be judged on AI-predicted behaviour based solely on their profiling, personality traits or characteristics, such as nationality, place of birth, place of residence, number of children, level of debt or type of car, without a reasonable suspicion of that person being involved in a criminal activity based on objective verifiable facts and without human assessment thereof. Therefore, risk assessments carried out with regard to natural persons in order to assess the likelihood of their offending or to predict the occurrence of an actual or potential criminal offence based solely on profiling them or on assessing their personality traits and characteristics should be prohibited. In any case, that prohibition does not refer to or touch upon risk analytics that are not based on the profiling of individuals or on the personality traits and characteristics of individuals, such as AI systems using risk analytics to assess the likelihood of financial fraud by undertakings on the basis of suspicious transactions or risk analytic tools to predict the likelihood of the localisation of narcotics or illicit goods by customs authorities, for example on the basis of known trafficking routes.

(43) The placing on the market, the putting into service for that specific purpose, or the use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage, should be prohibited because that practice adds to the feeling of mass surveillance and can lead to gross violations of fundamental rights, including the right to privacy.

(44) There are serious concerns about the scientific basis of AI systems aiming to identify or infer emotions, particularly as expression of emotions vary considerably across cultures and situations, and even within a single individual. Among the key shortcomings of such systems

are the limited reliability, the lack of specificity and the limited generalisability. Therefore, AI systems identifying or inferring emotions or intentions of natural persons on the basis of their biometric data may lead to discriminatory outcomes and can be intrusive to the rights and freedoms of the concerned persons. Considering the imbalance of power in the context of work or education, combined with the intrusive nature of these systems, such systems could lead to detrimental or unfavourable treatment of certain natural persons or whole groups thereof. Therefore, the placing on the market, the putting into service, or the use of AI systems intended to be used to detect the emotional state of individuals in situations related to the workplace and education should be prohibited. That prohibition should not cover AI systems placed on the market strictly for medical or safety reasons, such as systems intended for therapeutical use.

(45) Practices that are prohibited by Union law, including data protection law, non-discrimination law, consumer protection law, and competition law, should not be affected by this Regulation.

(46) High-risk AI systems should only be placed on the Union market, put into service or used if they comply with certain mandatory requirements. Those requirements should ensure that high-risk AI systems available in the Union or whose output is otherwise used in the Union do not pose unacceptable risks to important Union public interests as recognised and protected by Union law. On the basis of the New Legislative Framework, as clarified in the Commission notice 'The "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 applicable to one product, since the making available or putting into service can take place only when the product complies with all applicable Union harmonisation legislation. To ensure consistency and avoid unnecessary administrative burdens or costs, providers of a product that contains one or more high-risk AI systems, to which the requirements of this Regulation and of the Union harmonisation legislation listed in an annex to this Regulation apply, should have flexibility with regard to operational decisions on how to ensure compliance of a product that contains one or more AI systems with all applicable requirements of the Union harmonisation legislation in an optimal manner. AI systems identified as high-risk should be limited to those that have a significant harmful impact on the health, safety and fundamental rights of persons in the Union and such limitation should minimise any potential restriction to international trade.

(47) AI systems could have an adverse impact on the health and safety of persons, in particular when such systems operate as safety components of products. Consistent 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 otherwise compliant products find their way into the market, it is important that the safety risks that may be generated by a product as a whole due to its digital components, including AI systems, are duly prevented and mitigated. For instance, increasingly autonomous robots, whether in the context of manufacturing or personal

assistance and care should be able to safely operate and performs their functions in complex environments. Similarly, in the health sector where the stakes for life and health are particularly high, increasingly sophisticated diagnostics systems and systems supporting human decisions should be reliable and accurate.

(48) The extent of the adverse impact caused by the AI system on the fundamental rights protected by the Charter is of particular relevance when classifying an AI system as high risk. Those 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 of association, the right to non-discrimination, the right to education, consumer protection, workers' rights, the rights of persons with disabilities, gender equality, intellectual property rights, the right to an effective remedy and to a fair trial, the right of defence and the presumption of innocence, and the right to good administration. In addition to those rights, it is important to highlight the fact that children have specific rights as enshrined in Article 24 of the Charter and in the United Nations Convention on the Rights of the Child, further developed in the UNCRC General Comment No 25 as regards the digital environment, both of which require consideration of the children's vulnerabilities and provision of such protection and care as necessary for their well-being. The fundamental right to a high level of environmental protection enshrined in the Charter and implemented in Union policies should also be considered when assessing the severity of the harm that an AI system can cause, including in relation to the health and safety of persons.

(49) As regards high-risk AI systems that are safety components of products or systems, or which are themselves products or systems falling within the scope of Regulation (EC) No 300/2008 of the European Parliament and of the Council [24], Regulation (EU) No 167/2013 of the European Parliament and of the Council [25], Regulation (EU) No 168/2013 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 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 the Commission takes into account, on the basis of the technical and regulatory specificities of each sector, and without interfering with existing governance, conformity assessment and enforcement mechanisms and authorities established therein, the mandatory requirements for high-risk AI systems laid down in this Regulation when adopting any relevant delegated or implementing acts on the basis of those acts.

(50) As regards AI systems that are safety components of products, or which are themselves products, falling 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 undergoes the conformity assessment procedure with a third-party conformity assessment body pursuant to that relevant Union harmonisation legislation. In particular, such products are machinery, toys, lifts, equipment and protective systems intended

for use in potentially explosive atmospheres, radio equipment, pressure equipment, recreational craft equipment, cableway installations, appliances burning gaseous fuels, medical devices, *in vitro* diagnostic medical devices, automotive and aviation.

(51) The classification of an AI system as high-risk pursuant to this Regulation should not necessarily mean that the product whose safety component is the AI system, or the AI system itself as a product, is considered to be high-risk under the criteria established in the relevant Union harmonisation legislation that applies to the product. This is, in particular, the case for Regulations (EU) 2017/745 and (EU) 2017/746, where a third-party conformity assessment is provided for medium-risk and high-risk products.

(52) As regards stand-alone AI systems, namely high-risk AI systems other than those that are safety components of products, or that are themselves products, it is appropriate to classify them as high-risk if, in light of their intended purpose, they pose a high risk of harm to the health and safety or the fundamental rights of persons, taking into account both the severity of the possible harm and its probability of occurrence and they are used in a number of specifically pre-defined areas specified in this Regulation. The identification of those systems is based on the same methodology and criteria envisaged also for any future amendments of the list of high-risk AI systems that the Commission should be empowered to adopt, via delegated acts, to take into account the rapid pace of technological development, as well as the potential changes in the use of AI systems.

(53) It is also important to clarify that there may be specific cases in which AI systems referred to in pre-defined areas specified in this Regulation do not lead to a significant risk of harm to the legal interests protected under those areas because they do not materially influence the decision-making or do not harm those interests substantially. For the purposes of this Regulation, an AI system that does not materially influence the outcome of decision-making should be understood to be an AI system that does not have an impact on the substance, and thereby the outcome, of decision-making, whether human or automated. An AI system that does not materially influence the outcome of decision-making could include situations in which one or more of the following conditions are fulfilled. The first such condition should be that the AI system is intended to perform a narrow procedural task, such as an AI system that transforms unstructured data into structured data, an AI system that classifies incoming documents into categories or an AI system that is used to detect duplicates among a large number of applications. Those tasks are of such narrow and limited nature that they pose only limited risks which are not increased through the use of an AI system in a context that is listed as a high-risk use in an annex to this Regulation. The second condition should be that the task performed by the AI system is intended to improve the result of a previously completed human activity that may be relevant for the purposes of the high-risk uses listed in an annex to this Regulation. Considering those characteristics, the AI system provides only an additional layer to a human activity with consequently lowered risk. That condition would, for example, apply to AI systems that are intended to improve the language used in previously drafted documents, for example in relation to professional tone, academic style of language or by aligning text to

a certain brand messaging. The third condition should be that the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns. The risk would be lowered because the use of the AI system follows a previously completed human assessment which it is not meant to replace or influence, without proper human review. Such AI systems include for instance those that, given a certain grading pattern of a teacher, can be used to check *ex post* whether the teacher may have deviated from the grading pattern so as to flag potential inconsistencies or anomalies. The fourth condition should be that the AI system is intended to perform a task that is only preparatory to an assessment relevant for the purposes of the AI systems listed in an annex to this Regulation, thus making the possible impact of the output of the system very low in terms of representing a risk for the assessment to follow. That condition covers, inter alia, smart solutions for file handling, which include various functions from indexing, searching, text and speech processing or linking data to other data sources, or AI systems used for translation of initial documents. In any case, AI systems used in high-risk use-cases listed in an annex to this Regulation should be considered to pose significant risks of harm to the health, safety or fundamental rights if the AI system implies profiling within the meaning of Article 4, point (4) of Regulation (EU) 2016/679 or Article 3, point (4) of Directive (EU) 2016/680 or Article 3, point (5) of Regulation (EU) 2018/1725. To ensure traceability and transparency, a provider who considers that an AI system is not high-risk on the basis of the conditions referred to above should draw up documentation of the assessment before that system is placed on the market or put into service and should provide that documentation to national competent authorities upon request. Such a provider should be obliged to register the AI system in the EU database established under this Regulation. With a view to providing further guidance for the practical implementation of the conditions under which the AI systems listed in an annex to this Regulation are, on an exceptional basis, non-high-risk, the Commission should, after consulting the Board, provide guidelines specifying that practical implementation, completed by a comprehensive list of practical examples of use cases of AI systems that are high-risk and use cases that are not.

(54) As biometric data constitutes a special category of personal data, it is appropriate to classify as high-risk several critical-use cases of biometric systems, insofar as their use is permitted under relevant Union and national law. Technical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to biased results and entail discriminatory effects. The risk of such biased results and discriminatory effects is particularly relevant with regard to age, ethnicity, race, sex or disabilities. Remote biometric identification systems should therefore be classified as high-risk in view of the risks that they pose. Such a classification excludes AI systems intended to be used 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 and to confirm the identity of a natural person for the sole purpose of having access to a service, unlocking a device or having secure access to premises. In addition, AI systems intended to be used for biometric categorisation according to sensitive attributes or characteristics protected under Article 9(1) of Regulation (EU) 2016/679 on the basis of biometric data, in so far as these are not prohibited under this Regulation, and emotion

recognition systems that are not prohibited under this Regulation, should be classified as high-risk. Biometric systems which are intended to be used solely for the purpose of enabling cybersecurity and personal data protection measures should not be considered to be high-risk AI systems.

(55) As regards the management and operation of critical infrastructure, it is appropriate to classify as high-risk the AI systems intended to be used as safety components in the management and operation of critical digital infrastructure as listed in point (8) of the Annex to Directive (EU) 2022/2557, road traffic and the supply of water, gas, heating and electricity, since their failure or malfunctioning may put at risk the life and health of persons at large scale and lead to appreciable disruptions in the ordinary conduct of social and economic activities. Safety components of critical infrastructure, including critical digital infrastructure, are systems used to directly protect the physical integrity of critical infrastructure or the health and safety of persons and property but which are not necessary in order for the system to function. The failure or malfunctioning of such components might directly lead to risks to the physical integrity of critical infrastructure and thus to risks to health and safety of persons and property. Components intended to be used solely for cybersecurity purposes should not qualify as safety components. Examples of safety components of such critical infrastructure may include systems for monitoring water pressure or fire alarm controlling systems in cloud computing centres.

(56) The deployment of AI systems in education is important to promote high-quality digital education and training and to allow all learners and teachers to acquire and share the necessary digital skills and competences, including media literacy, and critical thinking, to take an active part in the economy, society, and in democratic processes. However, AI systems used in education or vocational training, in particular for determining access or admission, for assigning persons to educational and vocational training institutions or programmes at all levels, for evaluating learning outcomes of persons, for assessing the appropriate level of education for an individual and materially influencing the level of education and training that individuals will receive or will be able to access or for monitoring and detecting prohibited behaviour of students during tests should be classified as high-risk AI systems, since they may determine the educational and professional course of a person's life and therefore may affect that person's ability to secure a livelihood. When improperly designed and used, such systems may be particularly intrusive and may violate the right to education and training as well as the right not to be discriminated against and perpetuate historical patterns of discrimination, for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation.

(57) AI systems used in employment, workers management and access to self-employment, in particular for the recruitment and selection of persons, for making decisions affecting terms of the work-related relationship, promotion and termination of work-related contractual relationships, for allocating tasks on the basis of individual behaviour, personal traits or characteristics and for monitoring or evaluation of persons in work-related contractual

relationships, should also be classified as high-risk, since those systems may have an appreciable impact on future career prospects, livelihoods of those persons and workers' rights. Relevant work-related contractual relationships should, in a meaningful manner, involve employees and persons providing services through platforms as referred to in the Commission Work Programme 2021. Throughout the recruitment process and in the evaluation, promotion, or retention of persons in work-related contractual relationships, such systems may perpetuate historical patterns of discrimination, for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation. AI systems used to monitor the performance and behaviour of such persons may also undermine their fundamental rights to data protection and privacy.

(58) Another area in which the use of AI systems deserves special consideration is the access to and enjoyment of certain essential private and public services and benefits necessary for people to fully participate in society or to improve one's standard of living. In particular, natural persons applying for or receiving essential public assistance benefits and services from public authorities namely healthcare services, social security benefits, social services providing protection in cases such as maternity, illness, industrial accidents, dependency or old age and loss of employment and social and housing assistance, are typically dependent on those benefits and services and in a vulnerable position in relation to the responsible authorities. If AI systems are used for determining whether such benefits and services should be granted, denied, reduced, revoked or reclaimed by authorities, including whether beneficiaries are legitimately entitled to such benefits or services, those systems may have a significant impact on persons' livelihood and may infringe their fundamental rights, such as the right to social protection, non-discrimination, human dignity or an effective remedy and should therefore be classified as high-risk. Nonetheless, this Regulation should not hamper the development and use of innovative approaches in the public administration, which would stand to benefit from a wider use of compliant and safe AI systems, provided that those systems do not entail a high risk to legal and natural persons. In addition, AI systems used to evaluate the credit score or creditworthiness of natural persons should be classified as high-risk AI systems, since they determine those persons' access to financial resources or essential services such as housing, electricity, and telecommunication services. AI systems used for those purposes may lead to discrimination between persons or groups and may perpetuate historical patterns of discrimination, such as that based on racial or ethnic origins, gender, disabilities, age or sexual orientation, or may create new forms of discriminatory impacts. However, AI systems provided for by Union law for the purpose of detecting fraud in the offering of financial services and for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements should not be considered to be high-risk under this Regulation. Moreover, AI systems intended to be used for risk assessment and pricing in relation to natural persons for health and life insurance can also have a significant impact on persons' livelihood and if not duly designed, developed and used, can infringe their fundamental rights and can lead to serious consequences for people's life and health, including financial exclusion and discrimination. Finally, AI systems used to evaluate and classify

emergency calls by natural persons or to dispatch or establish priority in the dispatching of emergency first response services, including by police, firefighters and medical aid, as well as of emergency healthcare patient triage systems, should also be classified as high-risk since they make decisions in very critical situations for the life and health of persons and their property.

(59) Given their role and responsibility, actions by law enforcement authorities involving certain uses of AI systems are characterised by a significant degree of power imbalance and may lead to surveillance, arrest or deprivation of a natural person's liberty as well as other adverse impacts on fundamental rights guaranteed in the Charter. In particular, if the AI system is not trained with high-quality data, does not meet adequate requirements in terms of its performance, its accuracy or robustness, or is not properly designed and tested before being put on the market or otherwise put into service, it may single out people in a discriminatory or otherwise incorrect or unjust manner. Furthermore, the exercise of important procedural fundamental rights, such as the right to an effective remedy and to a fair trial as well as the right of defence and the presumption of innocence, could be hampered, in particular, where such AI systems are not sufficiently transparent, explainable and documented. It is therefore appropriate to classify as high-risk, insofar as their use is permitted under relevant Union and national law, a number of AI systems intended to be used in the law enforcement context where accuracy, reliability and transparency is particularly important to avoid adverse impacts, retain public trust and ensure accountability and effective redress. In view of the nature of the activities and the risks relating thereto, those 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 for assessing the risk of a natural person to become a victim of criminal offences, as polygraphs and similar tools, for the evaluation of the reliability of evidence in in the course of investigation or prosecution of criminal offences, and, insofar as not prohibited under this Regulation, for assessing the risk of a natural person offending or reoffending not solely on the basis of the profiling of natural persons or the assessment of personality traits and characteristics or the past criminal behaviour of natural persons or groups, for profiling in the course of detection, investigation or prosecution of criminal offences. AI systems specifically intended to be used for administrative proceedings by tax and customs authorities as well as by financial intelligence units carrying out administrative tasks analysing information pursuant to Union anti-money laundering law should not be classified as high-risk AI systems used by law enforcement authorities for the purpose of prevention, detection, investigation and prosecution of criminal offences. The use of AI tools by law enforcement and other relevant authorities should not become a factor of inequality, or exclusion. The impact of the use of AI tools on the defence rights of suspects should not be ignored, in particular the difficulty in obtaining meaningful information on the functioning of those systems and the resulting 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 persons who are often in particularly vulnerable position and who are dependent on the outcome of the actions of the competent public authorities. The accuracy, non-discriminatory nature and transparency of the AI systems used in those contexts are therefore particularly important to guarantee respect for the fundamental rights of the affected persons, in particular their rights to free movement, non-discrimination, protection of private life and personal data, international protection and good administration. It is therefore appropriate to classify as high-risk, insofar as their use is permitted under relevant Union and national law, AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies charged with tasks in the fields of migration, asylum and border control management as polygraphs and similar tools, for assessing certain risks posed by natural persons entering the territory of a Member State or applying for visa or asylum, for assisting competent public authorities for the examination, including related assessment of the reliability of evidence, of applications for asylum, visa and residence permits and associated complaints with regard to the objective to establish the eligibility of the natural persons applying for a status, for the purpose of detecting, recognising or identifying natural persons in the context of migration, asylum and border control management, with the exception of verification of travel documents. AI systems in the area of migration, asylum and border control management covered by this Regulation should comply with the relevant procedural requirements set by the Regulation (EC) No 810/2009 of the European Parliament and of the Council ([32]), the 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, in no circumstances, be used by Member States or Union institutions, bodies, offices or agencies as a means to circumvent their international obligations under the UN Convention relating to the Status of Refugees done at Geneva on 28 July 1951 as amended by the Protocol of 31 January 1967. Nor should they be used to in any way infringe on the principle of non-refoulement, or to deny safe and effective legal avenues into 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, considering their potentially significant impact on democracy, the rule of law, individual freedoms as well as the right to an effective remedy and to a fair trial. In particular, to address the risks of potential biases, errors and opacity, it is appropriate to qualify as high-risk AI systems intended to be used by a judicial authority or on its behalf to assist judicial authorities in researching and interpreting facts and the law and in applying the law to a concrete set of facts. AI systems intended to be used by alternative dispute resolution bodies for those purposes should also be considered to be high-risk when the outcomes of the alternative dispute resolution proceedings produce legal effects for the parties. The use of AI tools can support the decision-making power of judges or judicial independence, but should not replace it: the final decision-making must remain a human-driven activity. The classification of AI systems as high-risk should not, however, extend to AI systems intended

for purely ancillary administrative activities that do not affect the actual administration of justice in individual cases, such as anonymisation or pseudonymisation of judicial decisions, documents or data, communication between personnel, 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 referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda should be classified as high-risk AI systems with the exception of AI systems whose output natural persons are not directly exposed to, such as tools used to organise, optimise 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 the use of the system is lawful under other acts of Union law or under national law compatible with Union law, such as on the protection of personal data, on the use of polygraphs and similar tools or other systems to detect the emotional state of natural persons. Any such use should continue to occur solely in accordance with the applicable requirements resulting from the Charter and from the applicable acts of secondary Union law and national law. This Regulation should not be understood as providing for the legal ground for processing of personal data, including special categories of personal data, where relevant, unless it is specifically otherwise provided for in this Regulation.

(64) To mitigate the risks from high-risk AI systems placed on the market or put into service and to ensure a high level of trustworthiness, certain mandatory requirements should apply to high-risk AI systems, taking into account the intended purpose and the context of use of the AI system and according to the risk-management system to be established by the provider. The measures adopted by the providers to comply with the mandatory requirements of this Regulation should take into account the generally acknowledged state of the art on AI, be proportionate and effective to meet the objectives of this Regulation. Based on the New Legislative Framework, as clarified in Commission notice 'The "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 be applicable to one product, since the making available or putting into service can take place only when the product complies with all applicable Union harmonisation legislation. The hazards of AI systems covered by the requirements of this Regulation concern different aspects than the existing Union harmonisation legislation and therefore the requirements of this Regulation would complement the existing body of the Union harmonisation legislation. For example, machinery or medical devices products incorporating an AI system might present risks not addressed by the essential health and safety requirements set out in the relevant Union harmonised legislation, as that sectoral law does not deal with risks specific to AI systems. This calls for a simultaneous and complementary application of the various legislative acts. To ensure consistency and to avoid an unnecessary

administrative burden and unnecessary costs, providers of a product that contains one or more high-risk AI system, to which the requirements of this Regulation and of the Union harmonisation legislation based on the New Legislative Framework and listed in an annex to this Regulation apply, should have flexibility with regard to operational decisions on how to ensure compliance of a product that contains one or more AI systems with all the applicable requirements of that Union harmonised legislation in an optimal manner. That flexibility could mean, for example a decision by the provider to integrate a part of the necessary testing and reporting processes, information and documentation required under this Regulation into already existing documentation and procedures required under existing Union harmonisation legislation based on the New Legislative Framework and listed in an annex to this Regulation. This should not, in any way, undermine the obligation of the provider to comply with all the applicable requirements.

(65) The risk-management system should consist of a continuous, iterative process that is planned and run throughout the entire lifecycle of a high-risk AI system. That process should be aimed at identifying and mitigating the relevant risks of AI systems on health, safety and fundamental rights. The risk-management system should be regularly reviewed and updated to ensure its continuing effectiveness, as well as justification and documentation of any significant decisions and actions taken subject to this Regulation. This process should ensure that the provider identifies risks or adverse impacts and implements mitigation measures for the known and reasonably foreseeable risks of AI systems to the health, safety and fundamental rights in light of their intended purpose and reasonably foreseeable misuse, including the possible risks arising from the interaction between the AI system and the environment within which it operates. The risk-management system should adopt the most appropriate risk-management measures in light of the state of the art in AI. When identifying the most appropriate risk-management measures, the provider should document and explain the choices made and, when relevant, involve experts and external stakeholders. In identifying the reasonably foreseeable misuse of high-risk AI systems, the provider should cover uses of AI systems which, while not directly covered by the intended purpose and provided for in the instruction for use may nevertheless be reasonably expected to result from readily predictable human behaviour in the context of the specific characteristics and use of a particular AI system. Any known or foreseeable circumstances related to the use of the high-risk AI system in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to risks to the health and safety or fundamental rights should be included in the instructions for use that are provided by the provider. This is to ensure that the deployer is aware and takes them into account when using the high-risk AI system. Identifying and implementing risk mitigation measures for foreseeable misuse under this Regulation should not require specific additional training for the high-risk AI system by the provider to address foreseeable misuse. The providers however are encouraged to consider such additional training measures to mitigate reasonable foreseeable misuses as necessary and appropriate.

(66)Requirements should apply to high-risk AI systems as regards risk management, the quality and relevance of data sets used, technical documentation and record-keeping, transparency and the provision of information to deployers, human oversight, and robustness, accuracy and cybersecurity. Those requirements are necessary to effectively mitigate the risks for health, safety and fundamental rights. As no other less trade restrictive measures are reasonably available those requirements are not unjustified restrictions to trade.

(67)High-quality data and access to high-quality data plays a vital role in providing structure and in ensuring the performance of many AI systems, especially when techniques involving the training of models are used, with a view to ensure that the high-risk AI system performs as intended and safely and it does not become a source of discrimination prohibited by Union law. High-quality data sets for training, validation and testing require the implementation of appropriate data governance and management practices. Data sets for training, validation and testing, including the labels, should be relevant, sufficiently representative, and to the best extent possible free of errors 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 governance and management practices should include, in the case of personal data, transparency about the original purpose of the data collection. The data sets should also have the appropriate statistical properties, including as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used, with specific attention to the mitigation of possible biases in the data sets, that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited under Union law, especially where data outputs influence inputs for future operations (feedback loops). Biases can for example be inherent in underlying data sets, especially when historical data is being used, or generated when the systems are implemented in real world settings. Results provided by AI systems could be influenced by such inherent biases that are inclined to gradually increase and thereby perpetuate and amplify existing discrimination, in particular for persons belonging to certain vulnerable groups, including racial or ethnic groups. The requirement for the data sets to be to the best extent possible complete and free of errors should not affect the use of privacy-preserving 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 features, characteristics or elements that are particular to the specific geographical, contextual, behavioural or functional setting which the AI system is intended to be used. The requirements related to data governance can be complied with by having recourse to third parties that offer certified compliance services including verification of data governance, data set integrity, and data training, validation and testing practices, as far as compliance with the data requirements of this Regulation are ensured.

(68)For the development and assessment of high-risk AI systems, certain actors, such as providers, notified bodies and other relevant entities, such as European Digital Innovation Hubs, testing experimentation facilities and researchers, should be able to access and use high-quality data

sets within the fields of activities of those actors which are related to this Regulation. European common data spaces established by the Commission and the facilitation of data sharing between businesses and with government in the public interest will be instrumental to provide trustful, accountable and non-discriminatory access to high-quality data for the training, validation and testing of AI systems. For example, in health, the European health data space will facilitate non-discriminatory access to health data and the training of AI algorithms on those data sets, in a privacy-preserving, secure, timely, transparent and trustworthy manner, and with an appropriate institutional governance. Relevant competent authorities, including sectoral ones, providing or supporting the access to data may also support the provision of high-quality data for the training, validation and testing of AI systems.

(69) The right to privacy and to protection of personal data must be guaranteed throughout the entire lifecycle of the 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, are applicable when personal data are processed. Measures taken by providers to ensure compliance with those principles may include not only anonymisation and encryption, but also the use of technology that permits algorithms to be brought to the data and allows training of AI systems without the transmission between parties or copying of the raw or structured data themselves, without prejudice to the requirements on data governance provided for in this Regulation.

(70) In order to protect the right of others from the discrimination that might result from the bias in AI systems, the providers should, exceptionally, to the extent that it is strictly necessary for the purpose of ensuring bias detection and correction in relation to the high-risk AI systems, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons and following the application of all applicable conditions laid down under this Regulation in addition to the conditions laid down 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 substantial public interest within the meaning of Article 9(2), point (g) of Regulation (EU) 2016/679 and Article 10(2), point (g) of Regulation (EU) 2018/1725.

(71) Having comprehensible information on how high-risk AI systems have been developed and how they perform throughout their lifetime is essential to enable traceability of those systems, verify compliance with the requirements under this Regulation, as well as monitoring of their operations and post market monitoring. This requires keeping records and the availability of technical documentation, containing information which is necessary to assess the compliance of the AI system with the relevant requirements and facilitate post market monitoring. Such information should include the general characteristics, capabilities and limitations of the system, algorithms, data, training, testing and validation processes used as well as documentation on the relevant risk-management system and drawn in a clear and comprehensive form. The technical documentation should be kept up to date, appropriately throughout the lifetime of the AI system. Furthermore, high-risk AI systems should technically allow for the automatic recording of events, by means of logs, over the duration of the lifetime of the system.

(72) To address concerns related to opacity and complexity of certain AI systems and help deployers to fulfil their obligations under this Regulation, transparency should be required for high-risk AI systems before they are placed on the market or put it into service. High-risk AI systems should be designed in a manner to enable deployers to understand how the AI system works, evaluate its functionality, and comprehend its strengths and limitations. High-risk AI systems should be accompanied by appropriate information in the form of instructions of use. Such information should include the characteristics, capabilities and limitations of performance of the AI system. Those would cover information on possible known and foreseeable circumstances related to the use of the high-risk AI system, including deployer action that may influence system behaviour and performance, under which the AI system can lead to risks to health, safety, and fundamental rights, on the changes that have been pre-determined and assessed for conformity by the provider and on the relevant human oversight measures, including the measures to facilitate the interpretation of the outputs of the AI system by the deployers. Transparency, including the accompanying instructions for use, should assist deployers in the use of the system and support informed decision making by them. Deployers should, inter alia, be in a better position to make the correct choice of the system that they intend to use in light of the obligations applicable to them, be educated about the intended and precluded uses, and use the AI system correctly and as appropriate. In order to enhance legibility and accessibility of the information included in the instructions of use, where appropriate, illustrative examples, for instance on the limitations and on the intended and precluded uses of the AI system, should be included. Providers should ensure that all documentation, including the instructions for use, contains meaningful, comprehensive, accessible and understandable information, taking into account the needs and foreseeable knowledge of the target deployers. Instructions for use should be made available in a language which can be easily understood by target deployers, as determined by the Member State concerned.

(73) High-risk AI systems should be designed and developed in such a way that natural persons can oversee their functioning, ensure that they are used as intended and that their impacts are addressed over the system's lifecycle. To that end, appropriate human oversight measures should be identified by the provider of the system before its placing on the market or putting into service. In particular, where appropriate, such measures should guarantee that the system is subject to in-built operational constraints that cannot be overridden by the system itself and is responsive to the human operator, and that the natural persons to whom human oversight has been assigned have the necessary competence, training and authority to carry out that role. It is also essential, as appropriate, to ensure that high-risk AI systems include mechanisms to guide and inform a natural person to whom human oversight has been assigned to make informed decisions if, when and how to intervene in order to avoid negative consequences or risks, or stop the system if it does not perform as intended. Considering the significant consequences for persons in the case of an incorrect match by certain biometric identification systems, it is appropriate to provide for an enhanced human oversight requirement for those

systems so that no action or decision may be taken by the deployer on the basis of the identification resulting from the system unless this has been separately verified and confirmed by at least two natural persons. Those persons could be from one or more entities and include the person operating or using the system. This requirement should not pose unnecessary burden or delays and it could be sufficient that the separate verifications by the 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, this requirement should not apply where Union or national law considers the application of that requirement to be disproportionate.

(74) High-risk AI systems should perform consistently throughout their lifecycle and meet an appropriate level of accuracy, robustness and cybersecurity, in light of their intended purpose and in accordance with the generally acknowledged state of the art. The Commission and relevant organisations and stakeholders are encouraged to take due consideration of the mitigation of risks and the negative impacts of the AI system. The expected level of performance metrics should be declared in the accompanying instructions of use. Providers are urged to communicate that information to deployers in a clear and easily understandable way, free of 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 to help the transparency and fairness of commercial transactions. In that context, in cooperation with relevant stakeholders and organisation, such as metrology and benchmarking authorities, the Commission should encourage, as appropriate, the development of benchmarks and measurement methodologies for AI systems. In doing so, the Commission should take note and collaborate with international partners working on metrology and relevant measurement indicators relating to AI.

(75) Technical robustness is a key requirement for high-risk AI systems. They should be resilient in relation to harmful or otherwise undesirable behaviour that may result from limitations within the systems or the environment in which the systems operate (e.g. errors, faults, inconsistencies, unexpected situations). Therefore, technical and organisational measures should be taken to ensure robustness of high-risk AI systems, for example by designing and developing appropriate technical solutions to prevent or minimise harmful or otherwise undesirable behaviour. Those technical solution may include for instance mechanisms enabling the system to safely interrupt its operation (fail-safe plans) in the presence of certain anomalies or when operation takes place outside certain predetermined boundaries. Failure to protect against these risks could lead to safety impacts or negatively affect the fundamental rights, for example due to erroneous decisions or wrong or biased outputs generated by the AI system.

(76) Cybersecurity plays a crucial role in ensuring that AI systems are resilient against attempts to alter their use, behaviour, performance or compromise their security properties by malicious third parties exploiting the system's vulnerabilities. Cyberattacks against AI systems can

leverage AI specific 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. To ensure a level of cybersecurity appropriate to the risks, suitable measures, such as security controls, should therefore be taken by the providers of high-risk AI systems, also taking into account as 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 which fall 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 fulfilling the essential cybersecurity requirements set out in that regulation. When high-risk AI systems fulfil the essential requirements of a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, they should be deemed compliant with the cybersecurity requirements set out in this Regulation in so far as the achievement of those requirements is demonstrated in the EU declaration of conformity or parts thereof issued under that regulation. To that end, the assessment of the cybersecurity risks, associated to a product with digital elements classified as high-risk AI system according to this Regulation, carried out under a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, should consider risks to the cyber resilience of an AI system as regards attempts by unauthorised third parties to alter its use, behaviour or performance, including AI specific vulnerabilities such as data poisoning or adversarial attacks, as well as, as relevant, risks to fundamental rights as required by this Regulation.

(78) The conformity assessment procedure provided by this Regulation should apply in relation to the essential cybersecurity requirements of a product with digital elements covered 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 rule should not result in reducing the necessary level of assurance for critical products with digital elements covered by 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 rule, high-risk AI systems that fall within the scope of this Regulation and are also qualified as important and critical products with digital elements pursuant to 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 conformity assessment provisions of a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements insofar as the essential cybersecurity requirements of that regulation are concerned. In this case, for all the other aspects covered by this Regulation the respective

provisions on conformity assessment based on internal control set out in an annex to this Regulation should apply. Building on the knowledge and expertise of ENISA on the cybersecurity policy and tasks assigned to ENISA under the Regulation (EU) 2019/881 of the European Parliament and of the Council ([37]), the Commission should cooperate with ENISA on issues related to cybersecurity of AI systems.

(79) It is appropriate that a specific natural or legal person, defined as the provider, takes responsibility for the placing on the market or the putting into service of a high-risk AI system, regardless of whether that natural or legal person is the person who designed or developed the system.

(80) As signatories to the United Nations Convention on the Rights of Persons with Disabilities, the Union and the Member States are legally obliged to protect persons with disabilities from discrimination and 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 privacy for 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 everyone potentially affected by or using AI technologies, including persons with disabilities, in a way that takes full account of 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 should ensure compliance with these requirements by design. Therefore, the necessary measures should be integrated as much as possible into the design of the high-risk AI system.

(81) The provider should establish a sound quality management system, ensure the accomplishment of the required conformity assessment procedure, draw up the relevant documentation and establish a robust post-market monitoring system. Providers of high-risk AI systems that are subject to obligations regarding quality management systems under relevant sectoral Union law should have the possibility to include the elements of the quality management system provided for in this Regulation as part of the existing quality management system provided for in that other sectoral Union law. The complementarity between this Regulation and existing sectoral Union law should also be taken into account in future standardisation activities or guidance adopted by the Commission. Public authorities which put into service high-risk AI systems for their own use may adopt and implement the rules for the quality management system as part of the quality management system adopted at a national or regional level, as appropriate, taking into account the specificities of the sector and the competences and organisation of the public authority concerned.

(82) To enable enforcement of this Regulation and create a level playing field for operators, and, taking into account the different forms of making available of digital products, it is important to ensure that, under all circumstances, a person established in the Union can provide authorities with all the necessary information on the compliance of an AI system. Therefore,

prior to making their AI systems available in the Union, providers established in third countries should, by written mandate, appoint an authorised representative established in the Union. This authorised representative plays a pivotal role in ensuring the compliance of the high-risk AI systems placed on the market or put into service in the Union by those providers who are not established in the Union and in serving as their contact person established in the Union.

(83) In light of the nature and complexity of the value chain for AI systems and in line with the New Legislative Framework, it is essential to ensure legal certainty and facilitate the compliance with this Regulation. Therefore, it is necessary to clarify the role and the specific obligations of relevant operators along that value chain, such as importers and distributors who may contribute to the development of AI systems. In certain situations those operators could act in more than one role at the same time and should therefore fulfil cumulatively all relevant obligations associated with those roles. For example, an operator could act as a distributor and an importer at the same time.

(84) 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 to be a provider of a high-risk AI system and therefore assume all the relevant obligations. This would be the case if that party puts its name or trademark on a high-risk AI system already placed on the market or put into service, without prejudice to contractual arrangements stipulating that the obligations are allocated otherwise. This would also be the case if that party makes a substantial modification to a high-risk AI system that has already been placed on the market or has already been put into service in a way that it remains a high-risk AI system in accordance with this Regulation, or if it modifies the intended purpose of an AI system, including a general-purpose AI system, which has not been classified as high-risk and has already been placed on the market or put into service, in a way that the AI system becomes a high-risk AI system in accordance with this Regulation. Those provisions should apply without prejudice to more specific provisions established in certain Union harmonisation legislation based on the New Legislative Framework, together with which this Regulation should apply. For example, Article 16(2) of Regulation (EU) 2017/745, establishing that certain changes should not be considered to be modifications of a device that could affect its 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 by themselves or be components of other high-risk AI systems. Therefore, due to their particular nature and in order to ensure a fair sharing of responsibilities along the AI value chain, the providers of such systems should, irrespective of whether they may be used as high-risk AI systems as such by other providers or as components of high-risk AI systems and unless provided otherwise under this Regulation, closely cooperate with the providers of the relevant high-risk AI systems to enable their compliance with the relevant obligations under this Regulation and with the competent authorities established under this Regulation.

(86) Where, under the conditions laid down in this Regulation, the provider that initially placed the AI system on the market or put it into service should no longer be considered to be the provider for the purposes of this Regulation, and when that provider has not expressly excluded the change of the AI system into a high-risk AI system, the former provider should nonetheless closely cooperate and make available the necessary information and provide the reasonably expected technical access and other assistance that are required for the fulfilment of the obligations set out in this Regulation, in particular regarding the compliance with the conformity assessment of high-risk AI systems.

(87) In addition, where a high-risk AI system that is a safety component of a product which falls within the scope of Union harmonisation legislation based on the New Legislative Framework is not placed on the market or put into service independently from the product, the product manufacturer defined in that legislation should comply with the obligations of the provider established in this Regulation and should, in particular, ensure that the AI system embedded in the final product complies with the requirements of this Regulation.

(88) Along the AI value chain multiple parties often supply AI systems, tools and services but also components or processes that are incorporated by the provider into the AI system with various objectives, including the model training, model retraining, model testing and evaluation, integration into software, or other aspects of model development. Those parties have an important role to play in the value chain towards the provider of the high-risk AI system into which their AI systems, tools, services, components or processes are integrated, and should provide by written agreement this provider with the necessary information, capabilities, technical access and other assistance based on the generally acknowledged state of the art, in order to enable the provider to fully comply with the obligations set out in this Regulation, without compromising their own intellectual property rights or trade secrets.

(89) Third parties making accessible to the public tools, services, processes, or AI components other than general-purpose AI models, should not be mandated to comply with requirements targeting the responsibilities along the AI value chain, in particular towards the provider that has used or integrated them, when those tools, services, processes, or AI components are made accessible under a free and open-source licence. Developers of free and open-source tools, services, processes, or AI components other than general-purpose AI models should be encouraged to implement widely adopted documentation practices, such as model cards and data sheets, as a way to accelerate information sharing along the AI value chain, allowing the promotion of trustworthy AI systems in the Union.

(90) The Commission could develop and recommend voluntary model contractual terms between providers of high-risk AI systems and third parties that supply tools, services, components or processes that are used or integrated in high-risk AI systems, to facilitate the cooperation along the value chain. When developing voluntary model contractual terms, the Commission should also take into account possible contractual requirements applicable in specific sectors or business cases.

(91) Given the nature of AI systems and the risks to safety and fundamental rights possibly associated with their use, including as regards the need to ensure proper monitoring of the performance of an AI system in a real-life setting, it is appropriate to set specific responsibilities for deployers. Deployers should in particular take appropriate technical and organisational measures to ensure they use high-risk AI systems in accordance with the instructions of use and certain other obligations should be provided for with regard to monitoring of the functioning of the AI systems and with regard to record-keeping, as appropriate. Furthermore, deployers should ensure that the persons assigned to implement the instructions for use and human oversight as set out in this Regulation have the necessary competence, in particular an adequate level of AI literacy, training and authority to properly fulfil those tasks. Those obligations should be without prejudice to other deployer obligations in relation to high-risk AI systems under Union or national law.

(92) This Regulation is without prejudice to obligations for employers to inform or to inform and consult workers or their representatives under Union or national law and practice, including Directive 2002/14/EC of the European Parliament and of the Council ([39]), on decisions to put into service or use AI systems. It remains necessary to ensure information of workers and their representatives on the planned deployment of high-risk AI systems at the workplace where the conditions for those information or information and consultation obligations in other legal instruments are not fulfilled. Moreover, such information right is ancillary and necessary to the objective of protecting fundamental rights that underlies this Regulation. Therefore, an information requirement to that effect should be laid down in this Regulation, without affecting any existing rights of workers.

(93) Whilst risks related to AI systems can result from the way such systems are designed, risks can as well stem from how such AI systems are used. Deployers of high-risk AI system therefore play a critical role in ensuring that fundamental rights are protected, complementing the obligations of the provider when developing the AI system. Deployers are best placed to understand how the high-risk AI system will be used concretely and can therefore identify potential significant risks that were not foreseen in the development phase, due to a more precise knowledge of the context of use, the persons or groups of persons likely to be affected, including vulnerable groups. Deployers of high-risk AI systems listed in an annex to this Regulation also play a critical role in informing natural persons and should, when they make decisions or assist in making decisions related to natural persons, where applicable, inform the natural persons that they are subject to the use of the high-risk AI system. This information should include the intended purpose and the type of decisions it makes. The deployer should also inform the natural persons about their right to an explanation provided under this Regulation. With regard to high-risk AI systems used for law enforcement purposes, that obligation should be implemented in accordance with Article 13 of Directive (EU) 2016/680.

(94) Any processing of biometric data involved in the use of AI systems for biometric identification for the purpose of law enforcement needs to comply with Article 10 of Directive (EU)

2016/680, that allows 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, when authorised, also needs to respect the principles laid down in Article 4 (1) of Directive (EU) 2016/680 including lawfulness, fairness and transparency, purpose limitation, accuracy and storage limitation.

(95) Without prejudice to applicable Union law, in particular Regulation (EU) 2016/679 and Directive (EU) 2016/680, considering the intrusive nature of post-remote biometric identification systems, the use of post-remote biometric identification systems should be subject to safeguards. Post-remote biometric identification systems should always be used in a way that is proportionate, legitimate and strictly necessary, and thus targeted, in terms of the individuals to be identified, the location, temporal scope and based on a closed data set of legally acquired video footage. In any case, post-remote biometric identification systems should not be used in the framework of law enforcement to lead to indiscriminate surveillance. The conditions for post-remote biometric identification should in any case not provide a basis to circumvent the conditions of the prohibition and strict exceptions for real time remote biometric identification.

(96) In order to efficiently ensure that fundamental rights are protected, deployers of high-risk AI systems that are bodies governed by public law, or private entities providing public services and deployers 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 prior to putting it into use. Services important for individuals that are of public nature may also be provided by private entities. Private entities providing such public services are linked to tasks in the public interest such as in the areas of education, healthcare, social services, housing, administration of justice. The aim 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, identify measures to be taken in the case of a materialisation of those risks. The impact assessment should be performed prior to deploying 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 deployer's relevant processes in which the high-risk AI system will be used in line with its intended purpose, and should include a description of the period of time and frequency in which the system is intended to be used as well as of specific categories of natural persons and groups who are likely to be affected in the specific context of use. The assessment should also include the identification of specific risks of harm likely to have an impact on the fundamental rights of those persons or groups. While performing this assessment, the deployer should take into account information relevant to a proper assessment of the impact, including but not limited to the information given by the provider of the high-risk AI system in the instructions for use. In light of the risks identified, deployers should determine measures to be taken in the case of a materialisation of those risks, including for example governance arrangements in that specific context of use, such as arrangements for human oversight according to the instructions of use or, complaint handling and redress

procedures, as they could be instrumental in mitigating risks to fundamental rights in concrete use-cases. After performing that impact assessment, the deployer should notify the relevant market surveillance authority. Where appropriate, to collect relevant information necessary to perform the impact assessment, deployers of high-risk AI system, in particular when AI systems are used in the public sector, could involve relevant stakeholders, including the representatives of groups of persons likely to be affected by the AI system, independent experts, and civil society organisations in conducting such impact assessments and designing measures to be taken in the case of materialisation of the risks. The European Artificial Intelligence Office (AI Office) should develop a template for a questionnaire in order to facilitate compliance and reduce the administrative burden for deployers.

(97) The notion of general-purpose AI models should be clearly defined and set apart from the notion of AI systems to enable legal certainty. The definition should be based on the key functional characteristics of a general-purpose AI model, in particular the generality and the capability to competently perform a wide range of distinct tasks. These models are typically trained on large amounts of data, through various methods, such as self-supervised, unsupervised or reinforcement learning. General-purpose AI models may be placed on the market in various ways, including through libraries, application programming interfaces (APIs), as direct download, or as physical copy. These models may be further modified or fine-tuned into new models. Although AI models are essential components of AI systems, they do not constitute AI systems on their own. AI models require the addition of further components, such as for example a user interface, to become AI systems. AI models are typically integrated into and form part of AI systems. This Regulation provides specific rules for general-purpose AI models and for general-purpose AI models that pose systemic risks, which should apply also when these models are integrated or form part of an AI system. It should be understood that the obligations for the providers of general-purpose AI models should apply once the general-purpose AI models are placed on the market. When the provider of a general-purpose AI model integrates an own model into its own AI system that is made available on the market or put into service, that model should be considered to be placed on the market and, therefore, the obligations in this Regulation for models should continue to apply in addition to those for AI systems. The obligations laid down for models should in any case not apply when an own model is used for purely internal processes that are not essential for providing a product or a service to third parties and the rights of natural persons are not affected. Considering their potential significantly negative effects, the general-purpose AI models with systemic risk should always be subject to the relevant obligations under this Regulation. The definition should not cover AI models used before their placing on the market for the sole purpose of research, development and prototyping activities. This is without prejudice to the obligation to comply with this Regulation when, following such activities, a model is placed on the market.

(98) Whereas the generality of a model could, inter alia, also be determined by a number of parameters, models with at least a billion of parameters and trained with a large amount of

data using self-supervision at scale should be considered to display significant generality and to competently perform a wide range of distinctive tasks.

(99) Large generative AI models are a typical example for a general-purpose AI model, given that they allow for flexible generation of content, such as in the form of text, audio, images or video, that can readily accommodate a wide range of distinctive tasks.

(100) When a general-purpose AI model is integrated into or forms part of an AI system, this system should be considered to be general-purpose AI system when, due to this integration, this system has the capability to serve a variety of purposes. A general-purpose AI system can be used directly, or it may be 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 for a range of downstream systems, often provided by downstream providers that necessitate a good understanding of the models and their capabilities, both to enable the integration of such models into their products, and to fulfil their obligations under this or other regulations. Therefore, proportionate transparency measures should be laid down, including the drawing up and keeping up to date of documentation, and the provision of information on the general-purpose AI model for its usage by the downstream providers. Technical documentation should be prepared and kept up to date by the general-purpose AI model provider for the purpose of making it available, upon request, to the AI Office and the national competent authorities. The minimal set of elements to be included in such 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 light of evolving technological developments.

(102) Software and data, including models, released under a free and open-source licence that allows them to be openly shared and where users can freely access, use, modify and redistribute them or modified versions thereof, can contribute to research and innovation in the market and can provide significant growth opportunities for the Union economy. General-purpose AI models released under free and open-source licences should be considered to ensure high levels of transparency and openness if their parameters, including the weights, the information on the model architecture, and the information on model usage are made publicly available. The licence should be considered to be free and open-source also when it allows users to run, copy, distribute, study, change and improve software and data, including models under the condition that the original provider of the model is credited, the identical or comparable terms of distribution are respected.

(103) Free and open-source AI components covers the software and data, including models and general-purpose AI models, tools, services or processes of an AI system. Free and open-source AI components can be provided through different channels, including their development on open repositories. For the purposes of this Regulation, AI components that are provided against a price or otherwise monetised, including through the provision of technical support or other services, including through a software platform, related to the AI

component, or the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software, with the exception of transactions between microenterprises, should not benefit from the exceptions provided to free and open-source AI components. The fact of making AI components available through open repositories should not, in itself, constitute a monetisation.

(104) The providers of general-purpose AI models that are released under a free and open-source licence, and whose parameters, including the weights, the information on the model architecture, and the information on model usage, are made publicly available should be subject to exceptions as regards the transparency-related requirements imposed on general-purpose AI models, unless they can be considered to present a systemic risk, in which case the circumstance that the model is transparent and accompanied by an open-source license should not be considered to be a sufficient reason to exclude compliance with the obligations under this Regulation. In any case, given that the release of general-purpose AI models under free and open-source licence does not necessarily reveal substantial information on the data set used for the training or fine-tuning of the model and on how compliance of copyright law was thereby ensured, the exception provided for general-purpose AI models from compliance with the transparency-related requirements should not concern the obligation to produce a summary about the content used for model training and the obligation to put in place a policy to comply with Union copyright law, in particular to identify and comply with the reservation of rights pursuant to 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 innovation opportunities but also challenges to artists, authors, and other creators and the way their creative content is created, distributed, used and consumed. The development and training of such models require access to vast amounts of text, images, videos and other data. Text and data mining techniques may be used extensively in this context for the retrieval and analysis of such content, which may be protected by copyright and related rights. Any use of copyright protected content requires the authorisation of the rightsholder concerned unless relevant copyright exceptions and limitations apply. Directive (EU) 2019/790 introduced exceptions and limitations allowing reproductions and extractions of works or other subject matter, for the purpose of text and data mining, under certain conditions. Under these rules, rightsholders may choose to reserve their rights over their works or other subject matter to prevent text and data mining, unless this is done for the purposes of scientific research. Where the rights to opt out has been expressly reserved in an appropriate manner, providers of general-purpose AI models need to obtain an authorisation from rightsholders if they want to carry out text and data mining over such works.

(106) Providers that place general-purpose AI models on the Union market should ensure compliance with the relevant obligations in this Regulation. To that end, providers of general-purpose AI models should put in place a policy to comply with Union law on copyright and

related rights, in particular to identify and comply with the reservation of rights expressed by rightsholders 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 copyright-relevant acts underpinning the training of those general-purpose AI models take place. This is necessary to ensure a level playing field among providers of general-purpose AI models where no provider should be able to gain a competitive advantage in the Union market by applying lower copyright standards than those provided in the Union.

(107) In order to increase transparency on the data that is used in the pre-training and training of general-purpose AI models, including text and data protected by copyright law, it is adequate that providers of such models draw up and make publicly available a sufficiently detailed summary of the content used for training the general-purpose AI model. While taking into due account the need to protect trade secrets and confidential business information, this summary should be generally comprehensive in its scope instead of technically detailed 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 collections or sets that went into training the model, such as large private or public databases or data archives, and by providing a narrative explanation about other data sources used. It is appropriate for the AI Office to provide a template for the summary, which should be simple, effective, and allow the provider to provide the required summary in narrative form.

(108) With regard to the obligations imposed on providers of general-purpose AI models to put in place a policy to comply with Union copyright law and make publicly available a summary of the content used for the training, the AI Office should monitor whether the provider has fulfilled those obligations without verifying or proceeding to a work-by-work assessment of the training data in terms of copyright compliance. This Regulation does not affect the enforcement of copyright rules as provided for under Union law.

(109) Compliance with the obligations applicable to the providers of general-purpose AI models should be commensurate and proportionate to the type of model provider, excluding the need for compliance for persons who develop or use models for non-professional or scientific research purposes, who should nevertheless be encouraged to voluntarily comply 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 simplified ways of compliance for SMEs, including start-ups, that should not represent an excessive cost and not discourage the use of such models. In the case of a modification or fine-tuning of a model, the obligations for providers of general-purpose AI models should be limited to that modification or fine-tuning, for example by complementing the already existing technical documentation with information on the modifications, including new training data sources, as a means to comply with the value chain obligations provided in this Regulation.

(110) General-purpose AI models could pose systemic risks which include, but are not limited to, any actual or reasonably foreseeable negative effects in relation to major accidents, disruptions of critical sectors and serious consequences to public health and safety; any actual or reasonably foreseeable negative effects on democratic processes, public and economic security; the dissemination of illegal, false, or discriminatory content. Systemic risks should be understood to increase with model capabilities and model reach, can arise along the entire lifecycle of the model, and are influenced by conditions of misuse, model reliability, model fairness and model security, the level of autonomy of the model, its access to tools, novel or combined modalities, release and distribution strategies, the potential to remove guardrails and other factors. In particular, international approaches have so far identified the need to pay attention to risks from potential intentional misuse or unintended issues of control relating to alignment with human intent; chemical, biological, radiological, and nuclear risks, such as the ways in which barriers to entry can be lowered, including for weapons development, design acquisition, or use; offensive cyber capabilities, such as the ways in vulnerability discovery, exploitation, or operational use can be enabled; the effects of interaction and tool use, including for example the capacity to control physical systems and interfere with critical infrastructure; risks from models of making copies of themselves or 'self-replicating' or training other models; the ways in which models can give rise to harmful bias and discrimination with risks to individuals, communities or societies; the facilitation of disinformation or harming privacy with threats to democratic values and human rights; risk that a particular event could lead to a chain reaction with considerable negative effects that could affect up to an entire city, an entire domain 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 model with systemic risks. Since systemic risks result from particularly high capabilities, a general-purpose AI model should be considered to present systemic risks if it has high-impact capabilities, evaluated on the basis of appropriate technical tools and methodologies, or significant impact on the internal market due to its reach. High-impact capabilities in general-purpose AI models means capabilities that match or exceed the capabilities recorded in the most advanced general-purpose AI models. The full range of capabilities in a model could be better understood after its placing on the market or when deployers interact with the model. According to the state of the art at the time of 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 approximations for model capabilities. The cumulative amount of computation used for training includes the computation used across the activities and methods that are intended to enhance the capabilities of the model prior to deployment, such as pre-training, synthetic data generation and fine-tuning. Therefore, an initial threshold of floating point operations should be set, which, if met by a general-purpose AI model, leads to a presumption that the model is a general-purpose AI model with systemic risks. This threshold should be adjusted over time to reflect technological and industrial changes, such as algorithmic improvements

or increased hardware efficiency, and should be supplemented with benchmarks and indicators for model capability. To inform this, the AI Office should engage with the scientific community, industry, civil society and other experts. Thresholds, as well as tools and benchmarks for the assessment of high-impact capabilities, should be strong predictors of generality, its capabilities and associated systemic risk of general-purpose AI models, and could take into account the way the model will be placed on the market or the number of users it may affect. To complement this system, there should be a possibility for the Commission to take individual decisions designating a general-purpose AI model as a general-purpose AI model with systemic risk if it is found that such model has capabilities or an impact equivalent to those captured by the set threshold. That decision should be taken on the basis of an overall assessment of the criteria for the designation of a general-purpose AI model with systemic risk set out in an annex to this Regulation, such as quality or size of the training data set, number of business and end users, its input and output modalities, its level of autonomy and scalability, or the tools it has access to. Upon a reasoned request of a provider whose model has been designated as a general-purpose AI model with systemic risk, the Commission should take the request into account and may decide to reassess whether the general-purpose AI model can still be considered to present 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 models with systemic risk. The provider should notify the AI Office at the latest two weeks after the requirements are met or it becomes known that a general-purpose AI model will meet the requirements that lead to the presumption. This is especially relevant in relation to the threshold of floating point operations because training of general-purpose AI models takes considerable planning which includes the upfront allocation of compute resources and, therefore, providers of general-purpose AI models are able to know if their model would meet the threshold before the training is completed. In the context of that notification, the provider should be able to demonstrate that, because of its specific characteristics, a general-purpose AI model exceptionally does not present systemic risks, and that it thus should not be classified as a general-purpose AI model with systemic risks. That information is valuable for the AI Office to anticipate the placing on the market of general-purpose AI models with systemic risks and the providers can start to engage with the AI Office early on. That information is especially important with regard to general-purpose AI models that are planned to be released as open-source, given that, after the open-source model release, necessary measures to ensure compliance with the obligations under this Regulation may be more difficult to implement.

(113) If the Commission becomes aware of the fact that a general-purpose AI model meets the requirements to classify as a general-purpose AI model with systemic risk, which previously had either not been known or of which the relevant provider has failed to notify the Commission, the Commission should be empowered to designate it so. A system of qualified alerts should ensure that the AI Office is made aware by the scientific panel of general-

purpose AI models that should possibly be classified as general-purpose AI models with systemic risk, in addition to the monitoring activities of the AI Office.

(114) The providers of general-purpose AI models presenting systemic risks should be subject, in addition to the obligations provided for providers of general-purpose AI models, to obligations aimed at identifying and mitigating those risks and ensuring an adequate level of cybersecurity protection, regardless of whether it is provided as a standalone model or embedded in an AI system or a product. To achieve those objectives, this Regulation should require providers to perform the necessary model evaluations, in particular prior to its first placing on the market, including conducting and documenting adversarial testing of models, also, as appropriate, through internal or independent external testing. In addition, providers of general-purpose AI models with systemic risks should continuously assess and mitigate systemic risks, including for example by putting in place risk-management policies, such as accountability and governance processes, implementing post-market monitoring, taking appropriate measures along the entire model's 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 possible systemic risks. If, despite efforts to identify and prevent risks related to a general-purpose AI model that may present systemic risks, the development or use of the model causes a serious incident, the general-purpose AI model provider should without undue delay keep track of the incident and report any relevant information and possible corrective measures to the Commission and national competent authorities. Furthermore, providers should ensure an adequate level of cybersecurity protection for the model and its physical infrastructure, if appropriate, along the entire model lifecycle. Cybersecurity protection related to systemic risks associated with malicious use or attacks should duly consider accidental model leakage, unauthorised releases, circumvention of safety measures, and defence against cyberattacks, unauthorised access or model theft. That protection could be facilitated by securing model weights, algorithms, servers, and data sets, such as through operational security measures for information security, specific cybersecurity policies, adequate technical and established solutions, and cyber and physical access controls, appropriate to the relevant circumstances and the risks involved.

(116) The AI Office should encourage and facilitate the drawing up, review and adaptation of codes of practice, taking into account international approaches. All providers of general-purpose AI models could be invited to participate. To ensure that the codes of practice reflect the state of the art and duly take into account a diverse set of perspectives, the AI Office should collaborate with relevant national competent authorities, and could, where appropriate, consult with civil society organisations and other relevant stakeholders and experts, including the Scientific Panel, for the drawing up of such codes. Codes of practice should cover obligations for providers of general-purpose AI models and of general-purpose AI models presenting systemic risks. In addition, as regards systemic risks, codes of practice should help to establish a risk taxonomy of the type and nature of the systemic risks at Union level,

including their sources. Codes of practice should also be focused on specific risk assessment and mitigation measures.

(117) The codes of practice should represent a central tool for the proper compliance with the obligations provided for 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 approve a code of practice and give it a general validity within the Union, or, alternatively, to provide common rules for the implementation of the relevant obligations, if, by the time this Regulation becomes applicable, a code of practice cannot be finalised or is not deemed adequate by the AI Office. Once a harmonised standard is published and assessed as suitable to cover the relevant obligations by the AI Office, compliance with a European harmonised standard should grant providers the presumption of conformity. Providers of general-purpose AI models should furthermore be able to demonstrate compliance using alternative adequate means, if codes of practice or harmonised standards are not available, or they choose not to rely on those.

(118) This Regulation regulates AI systems and AI models by imposing certain requirements and obligations for relevant market actors that are placing them on the market, putting into service or use in the Union, thereby complementing obligations for providers of intermediary services that embed such systems or models into their services regulated by Regulation (EU) 2022/2065. To the extent that such systems or models are embedded into designated very large online platforms or very large online search engines, they are subject to the risk-management framework provided for in Regulation (EU) 2022/2065. Consequently, the corresponding obligations of this Regulation should be presumed to be fulfilled, unless significant systemic risks not covered by Regulation (EU) 2022/2065 emerge and are identified in such models. Within this framework, providers of very large online platforms and very large online search engines are obliged to assess potential systemic risks stemming from the design, functioning and use of their services, including how the design of algorithmic systems used in the service may contribute to such risks, as well as systemic risks stemming from potential misuses. Those providers are also obliged to take appropriate mitigating measures in observance of fundamental rights.

(119) Considering the quick pace of innovation and the technological evolution of digital services in scope of different instruments of Union law in particular having in mind the usage and the perception of their recipients, the 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 technology-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 performs searches of, in principle, all websites, then incorporates the results into its existing knowledge and uses the updated knowledge to generate a single output that combines different sources of information.

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

(121) Standardisation should play a key role to provide technical solutions to providers to ensure compliance with this Regulation, in line with the state of the art, to promote innovation as well as competitiveness and growth in the single market. Compliance with harmonised standards as defined in Article 2, point (1)(c), of Regulation (EU) No 1025/2012 of the European Parliament and of the Council ([41]), which are normally expected to reflect the state of the art, should be a means for providers to demonstrate conformity with the requirements of this Regulation. A balanced representation of interests involving all relevant stakeholders in the development of standards, in particular SMEs, consumer organisations and environmental and social stakeholders in accordance with Articles 5 and 6 of Regulation (EU) No 1025/2012 should therefore be encouraged. In order to facilitate compliance, the standardisation requests should be issued by the Commission without undue delay. When preparing the standardisation request, the Commission should consult the advisory forum and the Board in order to collect relevant expertise. However, in the absence of relevant references to harmonised standards, the Commission should be able to establish, via implementing acts, and after consultation of the advisory forum, common specifications for certain requirements under this Regulation. The common specification should be an exceptional fall back solution to facilitate the provider's obligation to comply with the requirements of this Regulation, when the standardisation request has not been accepted by any of the European standardisation organisations, or when the relevant harmonised standards insufficiently address fundamental rights concerns, or when the harmonised standards do not comply with the request, or when there are delays in the adoption of an appropriate harmonised standard. Where such a delay in the adoption of a harmonised standard is due to the technical complexity of that standard, this should be considered by the Commission before contemplating the establishment of common specifications. When developing common specifications, the Commission is encouraged to cooperate with international partners and international standardisation bodies.

(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 setting within which the AI system is intended to be used, should be presumed to comply with the relevant measure provided for under the requirement on data governance 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 been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to that Regulation and the references of which have been published in the *Official Journal of the European Union* should be presumed to comply with the cybersecurity requirement of this Regulation in so far as the cybersecurity certificate or statement of conformity or parts thereof cover the cybersecurity requirement of this Regulation. This remains without prejudice to the voluntary nature of that cybersecurity scheme.

(123) In order to ensure a high level of trustworthiness of high-risk AI systems, those systems should be subject to a conformity assessment prior to their placing on the market or putting into service.

(124) It is appropriate that, in order to minimise the burden on operators and avoid any possible duplication, for high-risk AI systems related to products which are covered by existing Union harmonisation legislation based on the New Legislative Framework, the compliance of those AI systems with the requirements of this Regulation should be assessed as part of the conformity assessment already provided for in that law. The applicability of the requirements of this Regulation should thus not affect the specific logic, methodology or general structure of conformity assessment under the relevant Union harmonisation legislation.

(125) Given the complexity of high-risk AI systems and the risks that are associated with them, it is important to develop an adequate conformity assessment procedure for high-risk AI systems involving notified bodies, so-called third party conformity assessment. However, given the current experience of professional pre-market certifiers in the field of product safety and the different nature of risks involved, it is appropriate to limit, at least in an initial phase of application of this Regulation, the scope of application of third-party conformity assessment for high-risk AI systems other than those related to products. Therefore, the conformity assessment of such systems should be carried out as a general rule by the provider under its own responsibility, with the only exception of AI systems intended to be used for biometrics.

(126) In order to carry out third-party conformity assessments when so required, notified bodies should be notified under this Regulation by the national competent authorities, provided that they comply with a set of requirements, in particular on independence, competence, absence of conflicts of interests and suitable cybersecurity requirements. Notification of those bodies should be sent by national competent authorities to the Commission and the other Member States by means of the electronic notification tool developed and managed by the Commission pursuant to Article R23 of Annex I to Decision No 768/2008/EC.

(127) In line with Union commitments under the World Trade Organization Agreement on Technical Barriers to Trade, it is adequate to facilitate the mutual recognition of conformity assessment results produced by competent conformity assessment bodies, independent of the

territory in which they are established, provided that those conformity assessment bodies established under the law of a third country meet the applicable requirements of this Regulation and the Union has concluded an agreement to that extent. In this context, the Commission should actively explore possible international instruments for that purpose and in particular pursue the conclusion of mutual recognition agreements with third countries.

(128) In line with the commonly established notion of substantial modification for products regulated by Union harmonisation legislation, it is appropriate that whenever a change occurs which may affect the compliance of a high-risk AI system with this Regulation (e.g. change of operating system or software architecture), or when the intended purpose of the system changes, that AI system should be considered to be a new AI system which should undergo a new conformity assessment. However, changes occurring to the algorithm and the performance of AI systems which continue to 'learn' after being placed on the market or put into service, namely automatically adapting how functions are carried out, should not constitute a substantial modification, provided that those changes have been pre-determined by the provider and assessed at the moment of the conformity assessment.

(129) High-risk AI systems should bear the CE marking to indicate their conformity with this Regulation so that they can move freely within the internal market. For high-risk AI systems embedded in a product, a physical CE marking should be affixed, and may be complemented by a digital CE marking. For high-risk AI systems only provided digitally, a digital CE marking should be used. Member States should not create unjustified obstacles to the placing on the market or the putting into service of high-risk AI systems that comply with the requirements laid down in this Regulation and bear the CE marking.

(130) Under certain conditions, rapid availability of innovative technologies may be crucial for health and safety of persons, the protection of the environment and climate change and for society as a whole. It is thus appropriate that under exceptional reasons of public security or protection of life and health of natural persons, environmental protection and the protection of key industrial and infrastructural assets, market surveillance authorities could authorise the placing on the market or the putting into service of AI systems which have not undergone a conformity assessment. In duly justified situations, as provided for in this Regulation, law enforcement authorities or civil protection authorities may put a specific high-risk AI system into service without the authorisation of the market surveillance authority, provided that such authorisation is requested during or after the use without undue delay.

(131) In order to facilitate the work of the Commission and the Member States in the AI field as well as to increase the transparency towards the public, providers of high-risk AI systems other than those related to products falling within the scope of relevant existing Union harmonisation legislation, as well as providers who consider that an AI system listed in the high-risk use cases in an annex to this Regulation is not high-risk on the basis of a derogation, should be required to register themselves and information about their AI system in an EU database, to be established and managed by the Commission. Before using an AI system

listed in the high-risk use cases in an annex to this Regulation, deployers of high-risk AI systems that are public authorities, agencies or bodies, should register themselves in such database and select the system that they envisage to use. Other deployers should be entitled to do so voluntarily. This section of the EU database should be publicly accessible, free of charge, the information should be easily navigable, understandable 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 relevant information to be submitted upon the registration of high-risk AI systems and on the use case of high-risk AI systems, set out in an annex to this Regulation, to which the high-risk AI systems correspond. Any substantial modification of high-risk AI systems should also be registered in the EU database. For high-risk AI systems in the area of law enforcement, migration, asylum and border control management, the registration obligations should be fulfilled in a secure non-public section of the EU database. Access to the secure non-public section should be strictly limited to the Commission as well as to market surveillance authorities with regard to their national section of that database. High-risk AI systems in the area 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, when deployed, the procedure for setting the database should include the development of functional specifications by the Commission and an independent audit report. The Commission should take into account cybersecurity risks when carrying out its tasks as data controller on the EU database. In order to maximise the availability and use of the EU database by the public, the EU database, including the information made available through it, should comply with requirements under the Directive (EU) 2019/882.

(132) Certain AI systems intended to interact with natural persons or to generate content may pose specific risks of impersonation or deception irrespective of whether they qualify as high-risk or not. In certain circumstances, the use of these systems should therefore be subject to specific transparency obligations without prejudice to the requirements and obligations for high-risk AI systems and subject to targeted exceptions to take into account the special need of law enforcement. In particular, natural persons should be notified that they are interacting with an AI system, unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect taking into account the circumstances and the context of use. When implementing that obligation, the characteristics of natural persons belonging to vulnerable groups due to their age or disability should be taken into account to the extent the AI system is intended to interact with those groups as well. Moreover, natural persons should be notified when they are exposed to AI systems that, by processing their biometric data, can identify or infer the emotions or intentions of those persons or assign them to specific categories. Such specific categories can relate to aspects such as sex, age, hair colour, eye colour, tattoos, personal traits, ethnic origin, personal preferences and interests. Such information and notifications should be provided in accessible formats for persons with disabilities.

(133) A variety of AI systems can generate large quantities of synthetic content that becomes increasingly hard for humans to distinguish from human-generated and authentic content. The wide availability and increasing capabilities of those systems have a significant impact on the integrity and trust in the information ecosystem, raising new risks of misinformation and manipulation at scale, fraud, impersonation and consumer deception. In light of those impacts, the fast technological pace and the need for new methods and techniques to trace origin of information, it is appropriate to require providers of those systems to embed technical solutions that enable marking in a machine readable format and detection that the output has been generated or manipulated by an AI system and not a human. Such techniques and methods should be sufficiently reliable, interoperable, effective and robust as far as this is technically feasible, taking into account available techniques or a combination of such techniques, such as watermarks, metadata identifications, cryptographic methods for proving provenance and authenticity of content, logging methods, fingerprints or other techniques, as may be appropriate. When implementing this obligation, providers should also take into account the specificities and the limitations of the different types of content and the relevant technological and market developments in the field, as reflected in the generally acknowledged state of the art. Such techniques and methods can be implemented at the level of the AI system or at the level of the AI model, including general-purpose AI models generating content, thereby facilitating fulfilment of this obligation by the downstream provider of the AI system. To remain proportionate, it is appropriate to envisage that this marking obligation should not cover AI systems performing primarily an assistive function for standard editing or AI systems not substantially altering the input data provided by the deployer or the semantics thereof.

(134) Further to the technical solutions employed by the providers of the AI system, deployers who use an AI system to generate or manipulate image, audio or video content that appreciably resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful (deep fakes), should also clearly and distinguishably disclose that the content has been artificially created or manipulated by labelling the AI output accordingly and disclosing its artificial origin. Compliance with this transparency obligation should not be interpreted as indicating that the use of the AI system or its output impedes the right to freedom of expression and the right to freedom of the arts and sciences guaranteed in the Charter, in particular where the content is part of an evidently creative, satirical, artistic, fictional or analogous work or programme, subject to appropriate safeguards for the rights and freedoms of third parties. In those cases, the transparency obligation for deep fakes set out in this Regulation is limited to disclosure of the existence of such generated or manipulated content in an appropriate manner that does not hamper the display or enjoyment of the work, including its normal exploitation and use, while maintaining the utility and quality of the work. In addition, it is also appropriate to envisage a similar disclosure obligation in relation to AI-generated or manipulated text to the extent it is published with the purpose of informing the public on matters of public interest unless the

AI-generated content has undergone a process of human review or editorial control and a natural or legal person holds editorial responsibility for the publication of the content.

(135) Without prejudice to the mandatory nature and full applicability of the transparency obligations, the Commission may also encourage and facilitate the drawing up of codes of practice at Union level to facilitate the effective implementation of the obligations regarding the detection and labelling of artificially generated or manipulated content, including to support practical arrangements for making, as appropriate, the detection mechanisms accessible and facilitating cooperation with other actors along the value chain, disseminating content or checking its authenticity and provenance to enable the public to effectively distinguish AI-generated content.

(136) The obligations placed on providers and deployers of certain AI systems in this Regulation to enable the detection and disclosure that the outputs of those systems are artificially generated or manipulated are particularly relevant to facilitate the effective implementation of Regulation (EU) 2022/2065. This applies in particular as regards the obligations of providers of very large online platforms or very large online search engines to identify and mitigate systemic risks that may arise from the dissemination of content that has been artificially generated or manipulated, in particular the risk of the actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, including through disinformation. The requirement to label content generated by AI systems under this Regulation is without prejudice to the obligation in Article 16(6) of Regulation (EU) 2022/2065 for providers of hosting services to process notices on illegal content received pursuant to Article 16(1) of that Regulation and should not influence the assessment and the decision on the illegality of the specific content. That assessment should be performed solely with reference to the rules governing the legality of the content.

(137) Compliance with the transparency obligations for the AI systems covered by this Regulation should not be interpreted as indicating that the use of the AI system or its output is lawful under this Regulation or other Union and Member State law and should be without prejudice to other transparency obligations for deployers of AI systems laid down in Union or national law.

(138) AI is a rapidly developing family of technologies that requires regulatory oversight and a safe and controlled space for experimentation, while ensuring responsible innovation and integration of appropriate safeguards and risk mitigation measures. To ensure a legal framework that promotes innovation, is future-proof and resilient to disruption, Member States should ensure that their national competent authorities establish at least one AI regulatory sandbox at national level to facilitate the development and testing of innovative AI systems under strict regulatory oversight before these systems are placed on the market or otherwise put into service. Member States could also fulfil this obligation through participating in already existing regulatory sandboxes or establishing jointly a sandbox with one or more Member States' competent authorities, insofar as this participation provides

equivalent level of national coverage for the participating Member States. AI regulatory sandboxes could be established in physical, digital or hybrid form and may accommodate physical as well as digital products. Establishing authorities should also ensure that the AI regulatory sandboxes have the adequate resources for their functioning, including financial and human resources.

(139) The objectives of the AI regulatory sandboxes should be to foster AI innovation by establishing a controlled experimentation and testing environment in the development and pre-marketing phase with a view to ensuring compliance of the innovative AI systems with this Regulation and other relevant Union and national law. Moreover, the AI regulatory sandboxes should aim to enhance legal certainty for innovators and the competent authorities' oversight and understanding of the opportunities, emerging risks and the impacts of AI use, to facilitate regulatory learning for authorities and undertakings, including with a view to future adaptions of the legal framework, to support cooperation and the sharing of best practices with the authorities involved in the AI regulatory sandbox, and to accelerate access to markets, including by removing barriers for SMEs, including start-ups. AI regulatory sandboxes should be widely available throughout the Union, and particular attention should be given to their accessibility for SMEs, including start-ups. The participation in the AI regulatory sandbox should focus on issues that raise legal uncertainty for providers and prospective providers to innovate, experiment with AI in the Union and contribute to evidence-based regulatory learning. The supervision of the AI systems in the AI regulatory sandbox should therefore cover their development, training, testing and validation before the systems are placed on the market or put into service, as well as the notion and occurrence of substantial modification that may require a new conformity assessment procedure. Any significant risks identified during the development and testing of such AI systems should result in adequate mitigation and, failing that, in the suspension of the development and testing process. Where appropriate, national competent authorities establishing AI regulatory sandboxes should cooperate with other relevant authorities, including those supervising the protection of fundamental rights, and could allow for the involvement of other actors within the AI ecosystem such as national or European standardisation organisations, notified bodies, testing and experimentation facilities, research and experimentation labs, European Digital Innovation Hubs and relevant stakeholder and civil society organisations. To ensure uniform implementation across the Union and economies of scale, it is appropriate to establish common rules for the AI regulatory sandboxes' implementation and a framework for cooperation between the relevant authorities involved in the supervision of the sandboxes. AI regulatory sandboxes established under this Regulation should be without prejudice to other law allowing for the establishment of other sandboxes aiming to ensure compliance with law other than this Regulation. Where appropriate, relevant competent authorities in charge of those other regulatory sandboxes should consider the benefits of using those sandboxes also for the purpose of ensuring compliance of AI systems with this Regulation. Upon agreement between the national competent authorities and the participants in the AI regulatory sandbox, testing in real world

conditions may also be operated and supervised in the framework of the AI regulatory sandbox.

(140) This Regulation should provide the legal basis for the providers and prospective providers in the AI regulatory sandbox to use personal data collected for other purposes for developing certain AI systems in the public interest within the AI regulatory sandbox, only under specified conditions, in accordance with Article 6(4) and Article 9(2), point (g), 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. All other obligations of data controllers and rights of data subjects under Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680 remain applicable. In particular, this Regulation should not provide a legal basis in the meaning of Article 22(2), point (b) of Regulation (EU) 2016/679 and Article 24(2), point (b) of Regulation (EU) 2018/1725. Providers and prospective providers in the AI regulatory sandbox should ensure appropriate safeguards and cooperate with the competent authorities, including by following their guidance and acting expeditiously and in good faith to adequately mitigate any identified significant risks to safety, health, and fundamental rights that may arise during the development, testing and experimentation in that sandbox.

(141) In order to accelerate the process of development and the placing on the market of the high-risk AI systems listed in an annex to this Regulation, it is important that providers or prospective providers of such systems may also benefit from a specific regime for testing those systems in real world conditions, without participating in an AI regulatory sandbox. However, in such cases, taking into account the possible consequences of such testing on individuals, it should be ensured that appropriate and sufficient guarantees and conditions are introduced by this Regulation for providers or prospective providers. Such guarantees should include, inter alia, requesting informed consent of natural persons to participate in testing in real world conditions, with the exception of law enforcement where the seeking of informed consent would prevent the AI system from being tested. Consent of subjects to participate in such testing under this Regulation is distinct from, and without prejudice to, consent of data subjects for the processing of their personal data under the relevant data protection law. It is also important to minimise the risks and enable oversight by competent authorities and therefore require prospective providers to have a real-world testing plan submitted to competent market surveillance authority, register the testing in dedicated sections in the EU database subject to some limited exceptions, set limitations on the period for which the testing can be done and require additional safeguards for persons belonging to certain vulnerable groups, as well as a written agreement defining the roles and responsibilities of prospective providers and deployers and effective oversight by competent personnel involved in the real world testing. Furthermore, it is appropriate to envisage additional safeguards to ensure that the predictions, recommendations or decisions of the AI system can be effectively reversed and disregarded and that personal data is protected and is deleted when the subjects have withdrawn their consent to participate in the testing without prejudice to their rights as data

subjects under the Union data protection law. As regards transfer of data, it is also appropriate to envisage that data collected and processed for the purpose of testing in real-world conditions should be transferred to third countries only where appropriate and applicable safeguards under Union law are implemented, in particular in accordance with bases for transfer of personal data under Union law on data protection, while for non-personal data appropriate safeguards are put in place in accordance with Union law, such as Regulations (EU) 2022/868 ([42]) and (EU) 2023/2854 ([43]) of the European Parliament and of the Council.

(142) To ensure that AI leads to socially and environmentally beneficial outcomes, Member States are encouraged to support and promote research and development of AI solutions in support of socially and environmentally beneficial outcomes, such as AI-based solutions to increase accessibility for persons with disabilities, tackle socio-economic inequalities, or meet environmental targets, by allocating sufficient resources, including public and Union funding, and, where appropriate and provided that the eligibility and selection criteria are fulfilled, considering in particular projects which pursue such objectives. Such projects should be based on the principle of interdisciplinary cooperation between AI developers, experts on inequality and non-discrimination, accessibility, consumer, environmental, and digital rights, as well as academics.

(143) In order to promote and protect innovation, it is important that the interests of SMEs, including start-ups, that are providers or deployers of AI systems are taken into particular account. To that end, Member States should develop initiatives, which are targeted at those operators, including on awareness raising and information communication. Member States should provide SMEs, including start-ups, that have a registered office or a branch in the Union, with priority access to the AI regulatory sandboxes provided that they fulfil the eligibility conditions and selection criteria and without precluding other providers and prospective providers to access the sandboxes provided the same conditions and criteria are fulfilled. Member States should utilise existing channels and where appropriate, establish new dedicated channels for communication with SMEs, including start-ups, deployers, other innovators and, as appropriate, local public authorities, to support SMEs throughout their development path by providing guidance and responding to queries about the implementation of this Regulation. Where appropriate, these channels should work together to create synergies and ensure homogeneity in their guidance to SMEs, including start-ups, and deployers. Additionally, Member States should facilitate the participation of SMEs and other relevant stakeholders in the standardisation development processes. Moreover, the specific interests and needs of providers that are SMEs, including start-ups, should be taken into account when notified bodies set conformity assessment fees. The Commission should regularly assess the certification and compliance costs for SMEs, including start-ups, through transparent consultations and should work with Member States to lower such costs. For example, translation costs related to mandatory documentation and communication with authorities may constitute a significant cost for providers and other operators, in particular those of a smaller scale. Member States should possibly ensure that one of the languages

determined and accepted by them for relevant providers' documentation and for communication with operators is one which is broadly understood by the largest possible number of cross-border deployers. 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 Board. Additionally, the Commission should complement Member States' efforts by providing a single information platform with easy-to-use information with regards to this Regulation for all providers and deployers, by organising appropriate communication campaigns to raise awareness about the obligations arising from this Regulation, and by evaluating and promoting the convergence of best practices in public procurement procedures in relation to AI systems. Medium-sized enterprises which until recently qualified as small enterprises within the meaning of the Annex to Commission Recommendation 2003/361/EC ([44]) should have access to those support measures, as those 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, all relevant Union funding programmes and projects, such as Digital Europe Programme, Horizon Europe, implemented by the Commission and the Member States at Union or national level should, as appropriate, contribute to the achievement of the objectives of this Regulation.

(145) In order to minimise the risks to implementation resulting from lack of knowledge and expertise in the market as well as to facilitate compliance of providers, in particular SMEs, including start-ups, and notified bodies with their obligations under this Regulation, 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 Union or national level should contribute to the implementation of this Regulation. Within their respective mission and fields of competence, the AI-on-demand platform, the European Digital Innovation Hubs and the testing and experimentation Facilities are able to provide in particular technical and scientific support to providers and notified bodies.

(146) Moreover, in light of the very small size of some operators and in order to ensure proportionality regarding costs of innovation, it is appropriate to allow microenterprises to fulfil one of the most costly obligations, namely to establish a quality management system, in a simplified manner which would reduce the administrative burden and the costs for those enterprises without affecting the level of protection and the need for compliance with the requirements for high-risk AI systems. The Commission should develop guidelines to specify the elements of the quality management system to be fulfilled in this simplified manner by microenterprises.

(147) It is appropriate that the Commission facilitates, to the extent possible, access to testing and experimentation facilities to bodies, groups or laboratories established or accredited pursuant to any relevant Union harmonisation legislation and which fulfil tasks in the context of

conformity assessment of products or devices covered by that Union harmonisation legislation. This is, in particular, the case as regards expert panels, expert laboratories and reference laboratories in the field of medical devices pursuant to Regulations (EU) 2017/745 and (EU) 2017/746.

(148) This Regulation should establish a governance framework that both allows to coordinate and support the application of this Regulation at national level, as well as build capabilities at Union level and integrate stakeholders in the field of AI. The effective implementation and enforcement of this Regulation require a governance framework that allows to coordinate and build up central expertise at Union level. The AI Office was established by Commission Decision ([45]) and has as its mission to develop Union expertise and capabilities in the field of AI and to contribute to the implementation of Union law on AI. Member States should facilitate the tasks of the AI Office with a view to support the development of Union expertise and capabilities at Union level and to strengthen the functioning of the digital single market. Furthermore, a Board composed of representatives of the Member States, a scientific panel to integrate the scientific community and an advisory forum to contribute stakeholder input to the implementation of this Regulation, at Union and national level, should be established. The development of Union expertise and capabilities should also include making use of existing resources and expertise, in particular through synergies with structures built up in the context of the Union level enforcement of other law 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) In order to facilitate a smooth, effective and harmonised implementation of this Regulation a Board should be established. The Board should reflect the various interests of the AI eco-system and be composed of representatives of the Member States. The Board should be responsible for a number of advisory tasks, including issuing opinions, recommendations, advice or contributing to guidance on matters related to the implementation of this Regulation, including on enforcement matters, technical specifications or existing standards regarding the requirements established in this Regulation and providing advice to the Commission and the Member States and their national competent authorities on specific questions related to AI. In order to give some flexibility to Member States in the designation of their representatives in the Board, such representatives may be any persons belonging to public entities who should have the relevant competences and powers to facilitate coordination at national level and contribute to the achievement of the Board's tasks. The Board should establish two standing sub-groups to provide a platform for cooperation and exchange among market surveillance authorities and notifying authorities on issues related, respectively, to market surveillance and notified bodies. The standing subgroup for market surveillance should act as the 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 standing subgroup for market surveillance by undertaking market evaluations or studies, in particular

with a view to identifying aspects of this Regulation requiring specific and urgent coordination among market surveillance authorities. The Board may establish other standing or temporary sub-groups as appropriate for the purpose of examining specific issues. The Board should also cooperate, as appropriate, with relevant Union bodies, experts groups and networks active in the context of relevant Union law, including in particular those active under relevant Union law on data, digital products and services.

(150) With a view to ensuring the involvement of stakeholders in the implementation and application of this Regulation, an advisory forum should be established to advise and provide technical expertise to the Board and the Commission. To ensure a varied and balanced stakeholder representation between commercial and non-commercial interest and, within the category of commercial interests, with regards to SMEs and other undertakings, the advisory forum should comprise inter alia industry, start-ups, SMEs, academia, civil society, including the social partners, as well as the Fundamental Rights Agency, ENISA, the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI).

(151) To support the implementation and enforcement of this Regulation, in particular the monitoring activities of the AI Office as regards general-purpose AI models, a scientific panel of independent experts should be established. The independent experts constituting the scientific panel should be selected on the basis of up-to-date scientific or technical expertise in the field of AI and should perform their tasks with impartiality, objectivity and ensure the confidentiality of information and data obtained in carrying out their tasks and activities. To allow the reinforcement of national capacities necessary for the effective enforcement of this Regulation, Member States should be able to request support from the pool of experts constituting the scientific panel for their enforcement activities.

(152) In order to support adequate enforcement as regards AI systems and reinforce the capacities of the Member States, Union AI testing support structures should be established and made available to the Member States.

(153) Member States hold a key role in the application and enforcement of this Regulation. In that respect, each Member State should designate at least one notifying authority and at least one market surveillance authority as national competent authorities for the purpose of supervising the application and implementation of this Regulation. Member States may decide to appoint any kind of public entity to perform the tasks of the national competent authorities within the meaning of this Regulation, in accordance with their specific national organisational characteristics and needs. In order to increase organisation efficiency on the side of Member States and to set a single point of contact vis-à-vis the public and other counterparts at Member State and Union levels, each Member State should designate a market surveillance authority to act as a single point of contact.

(154) The national competent authorities should exercise their powers independently, impartially and without bias, so as to safeguard the principles of objectivity of their activities and tasks and to ensure the application and implementation of this Regulation. The members of these authorities should refrain from any action incompatible with their duties and should be subject to confidentiality rules under this Regulation.

(155) In order to ensure that providers of high-risk AI systems can take into account the experience on the use of high-risk AI systems for improving their systems and the design and development process or can take any possible corrective action in a timely manner, all providers should have a post-market monitoring system in place. Where relevant, post-market monitoring should include an analysis of the interaction with other AI systems including other devices and software. Post-market monitoring should not cover sensitive operational data of deployers which are law enforcement authorities. This system is also key to ensure that the possible risks emerging from AI systems which continue to 'learn' after being placed on the market or put into service can be more efficiently and timely addressed. In this context, providers should also be required to have a system in place to report to the relevant authorities any serious incidents resulting from the use of their AI systems, meaning incident or malfunctioning leading to death or serious damage to health, serious and irreversible disruption of the management and operation of critical infrastructure, infringements of obligations under Union law intended to protect fundamental rights or serious damage to property or the environment.

(156) In order to ensure an appropriate and effective enforcement of the requirements and obligations set out by this Regulation, which is Union harmonisation legislation, the system of market surveillance and compliance of products established by Regulation (EU) 2019/1020 should apply in its entirety. Market surveillance authorities designated pursuant to this Regulation should have all enforcement powers laid down in this Regulation and in Regulation (EU) 2019/1020 and should exercise their powers and carry out their duties independently, impartially and without bias. Although the majority of 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 when they present a risk in accordance with this Regulation. Due to the specific nature of Union institutions, agencies and bodies falling within the scope of this Regulation, it is appropriate to designate the European Data Protection Supervisor as a competent market surveillance authority for them. This should be without prejudice to the designation of national competent authorities by the Member States. Market surveillance activities should not affect the ability of the supervised entities to carry out their tasks independently, when such independence is required by Union law.

(157) This Regulation is without prejudice to the competences, tasks, powers and independence of relevant national public authorities or bodies which supervise 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 set for ensuring adequate and timely enforcement against AI systems presenting a risk to health, safety and fundamental rights. The procedure for such AI systems presenting a risk should be applied to high-risk AI systems presenting a risk, prohibited systems which have been placed on the market, put into service or used in violation of the prohibited practices laid down in this Regulation and AI systems which have been made available in violation of the transparency requirements laid down in this Regulation and present a risk.

(158) Union financial services law includes internal governance and risk-management rules and requirements which are applicable to regulated financial institutions in the course of provision of those services, including when they make use of AI systems. In order to ensure coherent application and enforcement of the obligations under this Regulation and relevant rules and requirements of the Union financial services legal acts, the competent authorities for the supervision and enforcement of those legal acts, in particular competent authorities as defined in Regulation (EU) No 575/2013 of the European Parliament and of the Council (46) and Directives 2008/48/EC (47), 2009/138/EC (48), 2013/36/EU (49), 2014/17/EU (50) and (EU) 2016/97 (51) of the European Parliament and of the Council, should be designated, within their respective competences, as competent authorities for the purpose of supervising the implementation of this Regulation, including for market surveillance activities, as regards AI systems provided or used by regulated and supervised financial institutions unless Member States decide to designate another authority to fulfil these market surveillance tasks. Those competent authorities should have all powers under this Regulation and Regulation (EU) 2019/1020 to enforce the requirements and obligations of this Regulation, including powers to carry our *ex post* market surveillance activities that can be integrated, as appropriate, into their existing supervisory mechanisms and procedures under the relevant Union financial services law. It is appropriate to envisage that, when acting as market surveillance authorities under this Regulation, the national authorities responsible for the supervision of credit institutions regulated under Directive 2013/36/EU, which are participating in the Single Supervisory Mechanism established by Council Regulation (EU) No 1024/2013 (52), should report, without delay, to the European Central Bank any information identified in the course of their market surveillance activities that may be of potential interest for the European Central Bank's prudential supervisory tasks as specified in that Regulation. To further enhance the consistency between this Regulation and the rules applicable to credit institutions regulated under Directive 2013/36/EU, it is also appropriate to integrate some of the providers' procedural obligations in relation to risk management, post marketing monitoring and documentation into the existing obligations and procedures under Directive 2013/36/EU. In order to avoid overlaps, limited derogations should also be envisaged in relation to the quality management system of providers and the monitoring obligation placed on deployers of high-risk AI systems to the extent that these apply to credit institutions regulated by Directive 2013/36/EU. The same regime should apply to insurance and re-insurance

undertakings and insurance holding companies under Directive 2009/138/EC and the insurance intermediaries under Directive (EU) 2016/97 and other types of financial institutions subject to requirements regarding internal governance, arrangements or processes established pursuant to the relevant Union financial services law to ensure consistency and equal treatment in the financial sector.

(159) Each market surveillance authority for high-risk AI systems in the area of biometrics, as listed in an annex to this Regulation insofar as those systems are used for the purposes of law enforcement, migration, asylum and border control management, 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 that are being processed and to all information necessary for the performance of its tasks. The market surveillance authorities should be able to exercise their powers by acting with complete independence. Any limitations of their access to sensitive operational data under this Regulation should be without prejudice to the powers conferred to them by Directive (EU) 2016/680. No exclusion on disclosing data to national data protection authorities under this Regulation should affect the current or future powers of those authorities beyond the scope of this Regulation.

(160) The market surveillance authorities and the Commission should be able to propose joint activities, including joint investigations, to be conducted by market surveillance authorities or market surveillance authorities jointly with the Commission, that have the aim of promoting compliance, identifying non-compliance, raising awareness and providing guidance in relation to this Regulation with respect to specific categories of high-risk AI systems that are found to present a serious risk across two or more Member States. 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 for joint investigations.

(161) It is necessary to clarify the responsibilities and competences at Union and national level as regards AI systems that are built on general-purpose AI models. To avoid overlapping competences, where an AI system is based on a general-purpose AI model and the model and system are provided by the same provider, the supervision should take place at Union level through the AI Office, which should have the powers of a market surveillance authority within the meaning of Regulation (EU) 2019/1020 for this purpose. In all other cases, national market surveillance authorities remain responsible for the supervision of AI systems. However, for general-purpose AI systems that can be used directly by deployers for at least one purpose that is classified as high-risk, market surveillance authorities should cooperate with the AI Office to carry out evaluations of compliance and inform the Board and other market surveillance authorities accordingly. Furthermore, market surveillance authorities should be able to request assistance from the AI Office where the market surveillance authority is unable to conclude an investigation on a high-risk AI system because of its inability to access certain information related to the general-purpose AI model on which the high-risk AI system is built. In such cases, the procedure regarding mutual assistance in

cross-border cases in Chapter VI of Regulation (EU) 2019/1020 should apply *mutatis mutandis*.

(162) To make best use of the centralised Union expertise and synergies at Union level, the powers of supervision and enforcement of the obligations on providers of general-purpose AI models should be a competence of the Commission. The AI Office should be able to carry out all necessary actions to monitor the effective implementation of this Regulation as regards general-purpose AI models. It should be able to investigate possible infringements of the rules on providers of general-purpose AI models both on its own initiative, following the results of its monitoring activities, or upon request from market surveillance authorities in line with the conditions set out in this Regulation. To support effective monitoring of the AI Office, it should provide for the possibility that downstream providers lodge complaints about possible infringements of the rules on providers of general-purpose AI models and systems.

(163) With a view to complementing the governance systems for general-purpose AI models, the scientific panel should support the monitoring activities of the AI Office and may, in certain cases, provide qualified alerts to the AI Office which trigger follow-ups, such as investigations. This should be the case where the scientific panel has reason to suspect that a general-purpose AI model poses a concrete and identifiable risk at Union level. Furthermore, this should be the case where the scientific panel has reason to suspect that a general-purpose AI model meets the criteria that would lead to a classification as general-purpose AI model with systemic risk. To equip the scientific panel with the information necessary for the performance of those tasks, there should be a mechanism whereby the scientific panel can request the Commission to require documentation or information from a provider.

(164) The AI Office should be able to take the necessary actions to monitor the effective implementation of and compliance with the obligations for providers of general-purpose AI models laid down in this Regulation. The AI Office should be able to investigate possible infringements in accordance with the powers provided for in this Regulation, including by requesting documentation and information, by conducting evaluations, as well as by requesting measures from providers of general-purpose AI models. When conducting evaluations, in order to make use of independent expertise, the AI Office should be able to involve independent experts to carry out the evaluations on its behalf. Compliance with the obligations should be enforceable, inter alia, through requests to take appropriate measures, including risk mitigation measures in the case of identified systemic risks as well as restricting the making available on the market, withdrawing or recalling the model. As a safeguard, where needed beyond 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 apply *mutatis mutandis*, without prejudice to more specific procedural rights provided for by this Regulation.

(165) The development of AI systems other than high-risk AI systems in accordance with the requirements of this Regulation may lead to a larger uptake of ethical and trustworthy AI in the Union. Providers of AI systems that are not high-risk should be encouraged to create codes of conduct, including related governance mechanisms, intended to foster the voluntary application of some or all of the mandatory requirements applicable to high-risk AI systems, adapted in light of the intended purpose of the systems and the lower risk involved and taking into account the available technical solutions and industry best practices such as model and data cards. Providers and, as appropriate, deployers of all AI systems, high-risk or not, and AI models should also be encouraged to apply on a voluntary basis additional requirements related, for example, to the elements of the Union's Ethics Guidelines for Trustworthy AI, environmental sustainability, AI literacy measures, inclusive and diverse design and development of AI systems, including attention to vulnerable persons and accessibility to persons with disability, stakeholders' participation with the involvement, as appropriate, of relevant stakeholders such as business and civil society organisations, academia, research organisations, trade unions and consumer protection organisations in the design and development of AI systems, and diversity of the development teams, including gender balance. To ensure that the voluntary codes of conduct are effective, they should be based on clear objectives and key performance indicators to measure the achievement of those objectives. They should also be developed in an inclusive way, as appropriate, with the involvement of relevant stakeholders such as business and civil society organisations, academia, research organisations, trade unions and consumer protection organisation. The Commission may develop initiatives, including of a sectoral nature, to facilitate the lowering of technical barriers hindering cross-border exchange of data for AI development, including on data access infrastructure, semantic and technical interoperability of different types of data.

(166) It is important that AI systems related to products that are not high-risk in accordance with this Regulation and thus are not required to comply with the requirements set out for high-risk AI systems are nevertheless safe when 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] would apply as a safety net.

(167) In order to ensure trustful and constructive cooperation of competent authorities on Union and national level, all parties involved in the application of this Regulation should respect the confidentiality of information and data obtained in carrying out their tasks, in accordance with Union or national law. They should carry out their tasks and activities in such a manner as to protect, in particular, intellectual property rights, confidential business information and trade secrets, the effective implementation of this Regulation, public and national security interests, the integrity of criminal and administrative proceedings, and the integrity of classified information.

(168) Compliance with this Regulation should be enforceable by means of the imposition of penalties and other enforcement measures. Member States should take all necessary measures to ensure that the provisions of this Regulation are implemented, including by laying down effective, proportionate and dissuasive penalties for their infringement, and to respect the *ne bis in idem* principle. In order to strengthen and harmonise administrative penalties for infringement of this Regulation, the upper limits for setting the administrative fines for certain specific infringements should be laid down. When assessing the amount of the fines, Member States should, in each individual case, take into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and to the size of the provider, in particular if the provider is an SME, including a start-up. The European Data Protection Supervisor should have the power to impose fines on Union institutions, agencies and bodies falling within the scope of this Regulation.

(169) Compliance with the obligations on providers of general-purpose AI models imposed under this Regulation should be enforceable, inter alia, by means of fines. To that end, appropriate levels of fines should also be laid down for infringement of those obligations, including the failure to comply with measures requested by the Commission in accordance with this Regulation, subject to appropriate limitation periods in accordance with the principle of proportionality. All decisions taken by the Commission under this Regulation are subject to review by the Court of Justice of the European Union in accordance with the TFEU, including the unlimited jurisdiction of the Court of Justice with regard to penalties pursuant to Article 261 TFEU.

(170) Union and national law already provide effective remedies to 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 that has grounds to consider that there has been an infringement of this Regulation should be entitled to lodge a complaint to the relevant market surveillance authority.

(171) Affected persons should have the right to obtain an explanation where a deployer's decision is based mainly upon the output from certain high-risk AI systems that fall within the scope of this Regulation and where that decision produces legal effects or similarly significantly affects those persons in a way that they consider to have an adverse impact on their health, safety or fundamental rights. That explanation should be clear and meaningful and should provide a basis on which the affected persons are able to exercise their rights. The right to obtain an explanation should not apply to the use of AI systems for which exceptions or restrictions follow from Union or national law and should apply only to the extent this right is not already provided for under Union law.

(172) Persons acting as whistleblowers on the infringements of this Regulation should be protected under the Union law. Directive (EU) 2019/1937 of the European Parliament and of the

Council [54] should therefore apply to the reporting of infringements of this Regulation and the protection of persons reporting such infringements.

(173) In order to ensure that the regulatory framework can be adapted where 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 is not to be considered to be high-risk, the list of high-risk AI systems, the provisions regarding technical documentation, the content of the EU declaration of conformity the provisions regarding the conformity assessment procedures, the provisions establishing the high-risk AI systems to which the conformity assessment procedure based on assessment of the quality management system and assessment of the technical documentation should apply, the threshold, benchmarks and indicators, including by supplementing those benchmarks and indicators, in the rules for the classification of general-purpose AI models with systemic risk, the criteria for the designation of general-purpose AI models with systemic risk, the technical documentation for providers of general-purpose AI models and the transparency information for providers of general-purpose AI models. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down 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) Given the rapid technological developments and the technical expertise required to effectively apply this Regulation, the Commission should evaluate 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. Moreover, by 2 August 2028 and every four years thereafter, the Commission should evaluate and report to the European Parliament and to the Council on the need to amend the list of high-risk areas headings in the annex to this Regulation, the AI systems within the scope of the transparency obligations, the effectiveness of the supervision and governance system and the progress on the development of standardisation deliverables on energy efficient development of general-purpose AI models, including the need for further measures or actions. Finally, by 2 August 2028 and every three years thereafter, the Commission should evaluate the impact and effectiveness of voluntary codes of conduct to foster the application of the requirements provided for high-risk AI systems in the case of AI systems other than high-risk AI systems and possibly other 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 182/2011 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 uptake of human centric and trustworthy AI, while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection against harmful effects of AI systems in the Union and supporting innovation, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may 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 appropriate adaptation period for operators and avoid disruption to the market, including by ensuring continuity of the use of AI systems, it is appropriate that this Regulation applies to the high-risk AI systems that have been placed on the market or put into service before the general date of application thereof, 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 respect, the concept of significant change should be understood as equivalent in substance to the notion of substantial modification, which is used with regard only to high-risk AI systems pursuant to this Regulation. On an exceptional basis and in light of public accountability, operators of AI systems which are components of the large-scale IT systems established by the legal acts listed in an annex to this Regulation and operators of high-risk AI systems that are intended to be used by public authorities should, respectively, take the necessary steps to comply with the requirements of this Regulation by end of 2030 and by 2 August 2030.

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

(179) This Regulation should apply from 2 August 2026. However, taking into account the unacceptable risk associated with the use of AI in certain ways, the prohibitions as well as the general provisions of this Regulation should already apply from 2 February 2025. While the full effect of those prohibitions follows with the establishment of the governance and enforcement of this Regulation, anticipating the application of the prohibitions is important to take account of unacceptable risks and to have an effect on other procedures, such as in civil law. Moreover, the infrastructure related to the governance and the conformity assessment system should be operational before 2 August 2026, therefore the provisions on notified bodies and governance structure should apply from 2 August 2025. Given the rapid pace of technological advancements and adoption of general-purpose AI models, obligations for providers of general-purpose AI models should apply from 2 August 2025. Codes of practice should be ready by 2 May 2025 in view of enabling providers to demonstrate

compliance on time. The AI Office should ensure that classification rules and procedures are up to date in light of technological developments. In addition, Member States should lay down and notify to the Commission the rules on penalties, including administrative fines, and ensure that they are properly and effectively implemented by the date of application of this Regulation. Therefore the provisions on penalties should apply from 2 August 2025.

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

HAVE ADOPTED THIS REGULATION:

CHAPTER I
GENERAL PROVISIONS

Article 1

Subject matter`

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

2. This Regulation lays down:

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

(b) prohibitions of certain AI practices;

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

(d) harmonised transparency rules for certain AI systems;

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

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

(g) measures to support innovation, with a particular focus on SMEs, including start-ups.

Article 2

Scope

1. This Regulation applies to:

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

(b) deployers of AI systems that have their place of establishment or are located within the Union;

(c) providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union;

(d) importers and distributors of AI systems;

(e) product manufacturers placing on the market or putting into service an AI system together with their product and under their own name or trademark;

(f) authorised representatives of providers, which are not established in the Union;

(g) affected persons that are located in the Union.

2. For AI systems classified as high-risk AI systems in accordance with Article 6(1) related to products covered by the Union harmonisation legislation listed in Section B of Annex I, only Article 6(1), Articles 102 to 109 and Article 112 apply. Article 57 applies only in so far as the requirements for high-risk AI systems under this Regulation have been integrated in that Union harmonisation legislation.

3. This Regulation does not apply to areas outside the scope of Union law, and shall not, in any event, affect the competences of the Member States concerning national security, regardless of the type of entity entrusted by the Member States with carrying out tasks in relation to those competences.

This Regulation does not apply to AI systems where and in so far they 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 those activities.

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

4. This Regulation applies neither to public authorities in a third country nor to international organisations falling within the scope of this Regulation pursuant to paragraph 1, where those authorities or organisations use AI systems in the framework of international cooperation or agreements for law enforcement and judicial cooperation with the Union or with one or more Member States, provided that such a third country or international organisation provides adequate safeguards with respect to the protection of fundamental rights and freedoms of individuals.

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

6. This Regulation does not apply to AI systems or AI models, including their output, specifically developed and put into service for the sole purpose of scientific research and development.

7. Union law on the protection of personal data, privacy and the confidentiality of communications applies to personal data processed in connection with the rights and obligations laid down in this Regulation. This Regulation shall not affect Regulation (EU) 2016/679 or (EU) 2018/1725, or Directive 2002/58/EC or (EU) 2016/680, without prejudice to Article 10(5) and Article 59 of this Regulation.

8. This Regulation does not apply to any research, testing or development activity regarding AI systems or AI models prior to their being placed on the market or put into service. Such activities shall be conducted in accordance with applicable Union law. Testing in real world conditions shall not be covered by that exclusion.

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

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

11. This Regulation does not preclude the Union or Member States from maintaining or introducing laws, regulations or administrative provisions which are more favourable to workers in terms of protecting their rights in respect of the use of AI systems by employers, or from encouraging or allowing the application of collective agreements which are more favourable to workers.

12. This Regulation does not apply to AI systems released under free and open-source licences, unless they are placed on the market or put into service as high-risk AI systems or as an AI system that falls under Article 5 or 50.

Article 3

Definitions

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

(1)‘AI system’ means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;

(2)‘risk’ means the combination of the probability of an occurrence of harm and the severity of that harm;

(3)‘provider’ means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge;

(4)‘deployer’ means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity;

(5)‘authorised representative’ means a natural or legal person located or established in the Union who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation;

(6)‘importer’ means a natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country;

(7)‘distributor’ means a natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market;

(8)‘operator’ means a provider, product manufacturer, deployer, authorised representative, importer or distributor;

(9)‘placing on the market’ means the first making available of an AI system or a general-purpose AI model on the Union market;

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

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

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

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

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

(15)‘instructions for use’ means the information provided by the provider to inform the deployer of, in particular, an AI system’s intended purpose and proper use;

(16)‘recall of an AI system’ means any measure aiming to achieve the return to the provider or taking out of service or disabling the use of an AI system made available to deployers;

(17)‘withdrawal of an AI system’ means any measure aiming to prevent an AI system in the supply chain being made available on the market;

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

(19)‘notifying authority’ means the national authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring;

(20)‘conformity assessment’ means the process of demonstrating whether the requirements set out in Chapter III, Section 2 relating to a high-risk AI system have been fulfilled;

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

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

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

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

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

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

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

(28)‘common specification’ means a set of technical specifications as defined in Article 2, point (4) of Regulation (EU) No 1025/2012, providing means to comply with certain requirements established under this Regulation;

(29)‘training data’ means data used for training an AI system through fitting its learnable parameters;

(30)‘validation data’ means data used for providing an evaluation of the trained AI system and for tuning its non-learnable parameters and its learning process in order, inter alia, to prevent underfitting or overfitting;

(31)‘validation data set’ means a separate data set or part of the training data set, either as a fixed or variable split;

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

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

(34)‘biometric data’ means personal data resulting from specific technical processing 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 human features for the purpose of establishing the identity of a natural person by comparing biometric data of that individual to biometric data of individuals stored 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 to previously provided biometric data;

(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 related to activities of 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 for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data;

(40)‘biometric categorisation system’ means an AI system for the purpose of assigning natural persons to 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 for the purpose of identifying natural persons, without their active involvement, typically at a distance through the

comparison of a person's biometric data with the biometric data contained in a reference database;

(42) 'real-time remote biometric identification system' means a remote biometric identification system, whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay, comprising not only instant identification, but also limited short delays in order to avoid circumvention;

(43) 'post-remote biometric identification system' means a remote biometric identification system other than a real-time remote biometric identification system;

(44) 'publicly accessible space' means any publicly or privately owned physical place accessible to an undetermined number of natural persons, regardless of whether certain conditions for access may apply, and regardless of the potential capacity restrictions;

(45) 'law enforcement authority' means:

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

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

(46) 'law enforcement' means activities carried out by law enforcement authorities or on their behalf 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 Commission's function of contributing to the implementation, monitoring and supervision of AI systems and general-purpose AI models, and AI governance, provided for in 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; as regards AI systems put into service or used by Union institutions, agencies, offices and bodies, references to national competent authorities or market surveillance authorities in this Regulation shall be construed as references to the European Data Protection Supervisor;

(49) 'serious incident' means an incident or malfunctioning of an AI system that directly or indirectly leads to any of the following:

(a) the death of a person, or serious harm to a person's health;

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

(c)the infringement of obligations under Union law intended to protect fundamental rights;

(d) serious harm to property or the environment;

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

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

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

(53)‘real-world testing plan’ means a document that describes the objectives, methodology, geographical, population and temporal scope, monitoring, organisation and conduct of testing in real-world conditions;

(54)‘sandbox plan’ means a document agreed between the participating provider and the competent authority describing the objectives, conditions, timeframe, methodology and requirements for the activities carried out within the sandbox;

(55)‘AI regulatory sandbox’ means a controlled framework set up by a competent authority which offers providers or prospective providers of AI systems the possibility to develop, train, validate and test, where appropriate in real-world conditions, an innovative AI system, pursuant to a sandbox plan for a limited time under regulatory supervision;

(56)‘AI literacy’ means skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause;

(57)‘testing in real-world conditions’ means the temporary testing of an AI system for its intended purpose in real-world conditions outside a laboratory or otherwise simulated environment, with a view to gathering reliable and robust data and to assessing and verifying the conformity of the AI system with the requirements of this Regulation and it does not qualify as placing the AI system on the market or putting it into service within the meaning of this Regulation, provided that all the conditions laid down in Article 57 or 60 are fulfilled;

(58)‘subject’, for the purpose of real-world testing, means a natural person who participates in testing in real-world conditions;

(59)‘informed consent’ means a subject’s freely given, specific, unambiguous and voluntary expression of his or her willingness to participate in a particular testing in real-world conditions, after having been informed of all aspects of the testing that are relevant to the subject’s decision to participate;

(60)‘deep fake’ means AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful;

(61) ‘widespread infringement’ means any act or omission contrary to Union law protecting the interest of individuals, which:

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

(i) the act or omission originated or took place;

(ii) the provider concerned, or, where applicable, its authorised representative is located or established; or

(iii) the deployer is established, when the infringement is committed by the deployer;

(b) has caused, causes or is likely to cause harm to the collective interests of individuals and has common features, including the same unlawful practice or the same interest being infringed, and is occurring concurrently, committed by the same operator, in at least three Member States;

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

(63) ‘general-purpose AI model’ means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market;

(64) ‘high-impact capabilities’ means capabilities that match or exceed the capabilities recorded in the most advanced general-purpose AI models;

(65) ‘systemic risk’ means a risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain;

(66) ‘general-purpose AI system’ means an AI system which is based on a general-purpose AI model and which has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems;

(67) ‘floating-point operation’ means any mathematical operation or assignment involving floating-point numbers, which are a subset of the real numbers typically represented on computers by an integer of fixed precision scaled by an integer exponent of a fixed base;

(68) ‘downstream provider’ means a provider of an AI system, including a general-purpose AI system, which integrates an AI model, regardless of whether the AI model is provided by

themselves and vertically integrated or provided by another entity based on contractual relations.

Article 4

AI literacy

Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

CHAPTER II
PROHIBITED AI PRACTICES

Article 5

Prohibited AI practices

1. The following AI practices shall be prohibited:

(a) the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm;

(b) the placing on the market, the putting into service or the use of an AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm;

(c) the placing on the market, the putting into service or the use of AI systems for the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics, with the social score leading to either or both of the following:

(i) detrimental or unfavourable treatment of certain natural persons or groups of persons in social contexts that are unrelated to the contexts in which the data was originally generated or collected;

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

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

(e) the placing on the market, the putting into service for this specific purpose, or the use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;

(f) the placing on the market, the putting into service for this specific purpose, or the use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons;

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

(h) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the following objectives:

(i) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons;

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

(iii) the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years.

Point (h) of the first subparagraph is without prejudice to Article 9 of Regulation (EU) 2016/679 for the processing of biometric data for purposes other than law enforcement.

2. The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement for any of the objectives referred to in paragraph 1, first subparagraph, point (h), shall be deployed for the purposes set out in that point only to confirm the identity of the specifically targeted individual, and it shall take into account the following elements:

(a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm that would be caused if the system were not used;

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

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

3. For the purposes of paragraph 1, first subparagraph, point (h) and paragraph 2, each use for the purposes of law enforcement of a 'real-time' remote biometric identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or an independent administrative authority whose decision is binding of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 5. However, in a duly justified situation of urgency, the use of such system may be commenced without an authorisation provided that such authorisation is requested without undue delay, at the latest within 24 hours. If such authorisation is rejected, the use shall be stopped with immediate effect and all the data, as well as the results and outputs of that use shall be immediately discarded and deleted.

The competent judicial authority or an independent administrative authority whose decision is binding shall grant the authorisation only where it is satisfied, on the basis of objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system concerned is necessary for, and proportionate

to, achieving one of the objectives specified in paragraph 1, first subparagraph, point (h), as identified in the request and, in particular, remains limited to what is strictly necessary concerning the period of time as well as the geographic and personal scope. In deciding on the request, that authority shall take into account the elements referred to in paragraph 2. No decision that produces an adverse legal effect on a person may be taken based solely on the output of the 'real-time' remote biometric identification system.

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

5. A Member State may decide to provide for the possibility to fully or partially authorise the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement within the limits and under the conditions listed in paragraph 1, first subparagraph, point (h), and paragraphs 2 and 3. Member States concerned shall lay down in their national law the necessary detailed rules for the request, issuance and exercise of, as well as supervision and reporting relating to, the authorisations referred to in paragraph 3. Those rules shall also specify in respect of which of the objectives listed in paragraph 1, first subparagraph, point (h), including which of the criminal offences referred to in point (h)(iii) thereof, the competent authorities may be authorised to use those systems for the purposes of law enforcement. Member States shall notify those rules to the Commission at the latest 30 days following the adoption thereof. Member States may introduce, in accordance with Union law, more restrictive laws on the use of remote biometric identification systems.

6. National market surveillance authorities and the national data protection authorities of Member States that have been notified of the use of 'real-time' remote biometric identification systems in publicly accessible spaces for law enforcement purposes pursuant to paragraph 4 shall submit to the Commission annual reports on such use. For that purpose, the Commission shall provide Member States and national market surveillance and data protection authorities with a template, including information on the number of the decisions taken by competent judicial authorities or an independent administrative authority whose decision is binding upon requests for authorisations in accordance with paragraph 3 and their result.

7. The Commission shall publish annual reports on the use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes, based on aggregated data in 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 law enforcement activities.

8. This Article shall not affect the prohibitions that apply where an AI practice infringes other Union law.

CHAPTER III
HIGH-RISK AI SYSTEMS

SECTION 1
Classification of AI systems as high-risk

Article 6

Classification rules for high-risk AI systems

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

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

(b) the product whose safety component pursuant to point (a) is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment, with a view to the placing on the market or the putting into service of that product pursuant to the Union harmonisation legislation 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 be considered to be high-risk.

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

The first subparagraph shall apply where any of the following conditions is fulfilled:

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

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

(c) the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or

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

Notwithstanding the first subparagraph, an AI system referred to in Annex III shall always be considered to be high-risk where the AI system performs profiling of natural persons.

4. A provider who 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. Such provider shall be subject to the registration obligation set out in Article 49(2). Upon request of national competent authorities, the provider shall provide the documentation of the assessment.

5. The Commission shall, after consulting the European Artificial Intelligence Board (the 'Board'), and no later than 2 February 2026, provide guidelines specifying the practical implementation of this Article in line with Article 96 together with a comprehensive list of practical examples of use cases of AI systems that are high-risk and not high-risk.

6. The Commission is empowered to adopt delegated acts in accordance with Article 97 in order to amend paragraph 3, second subparagraph, of this Article by adding new conditions to those laid down therein, or by modifying them, where there is concrete and reliable evidence of the existence of AI systems that fall under the scope of Annex III, but 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 in order to amend paragraph 3, second subparagraph, of this Article by deleting any of the conditions laid down therein, where there is concrete and reliable evidence that this is necessary to maintain the level of protection of health, safety and fundamental rights provided for by this Regulation.

8. Any amendment to the conditions laid down in paragraph 3, second subparagraph, adopted in accordance with paragraphs 6 and 7 of this Article shall not decrease the overall level of protection of health, safety and fundamental rights provided for by this Regulation and shall ensure consistency with the delegated acts adopted pursuant to Article 7(1), and take account of market and technological developments.

Article 7

Amendments to Annex III

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

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

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

2. When assessing the condition under paragraph 1, point (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 used or is likely to be used;

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

(d)the extent to which the AI system acts autonomously and the possibility for a human to override a decision or recommendations that may lead to potential harm;

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

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

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

(h)the extent to which there is an imbalance of power, or the persons who are potentially harmed or suffer an adverse impact are in a vulnerable position in relation to the deployer of an AI system, in particular due to status, authority, knowledge, economic or social circumstances, or age;

(i)the extent to which the outcome produced involving an AI system is easily corrigible or reversible, taking into account the technical solutions available to correct or reverse it, whereby outcomes having an adverse impact on health, safety or fundamental rights, shall not be considered to be easily corrigible or reversible;

(j)the magnitude and likelihood of benefit of the deployment of the AI system for individuals, groups, or society at large, including possible improvements in product safety;

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

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

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

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

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

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

SECTION 2

Requirements for high-risk AI systems

Article 8

Compliance with the requirements

1. High-risk AI systems shall comply with the requirements laid down in this Section, taking into account their intended purpose as well as the generally acknowledged state of the art on AI and AI-related technologies. The risk management system referred to in Article 9 shall be taken into account when ensuring compliance with those requirements.

2. Where a product contains an AI system, to which the requirements of this Regulation as well as requirements of the Union harmonisation legislation listed in Section A of Annex I apply, providers shall be responsible for ensuring that their product is fully compliant with all applicable requirements under applicable Union harmonisation legislation. In ensuring the 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, providers shall have a choice of integrating, as appropriate, the necessary testing and reporting processes, information and documentation they provide with regard to their product into documentation and procedures that already exist and are required under the Union harmonisation legislation listed in Section A of Annex I.

Article 9

Risk management system

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

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

(a) the identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can 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 evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose, and under conditions of reasonably foreseeable misuse;

(c) the evaluation of other risks possibly arising, based on the analysis of data gathered from the post-market monitoring system referred to in Article 72;

(d) the adoption of appropriate and targeted risk management measures designed to address the risks identified pursuant to point (a).

3. The risks referred to in this Article shall concern only those which may be reasonably mitigated or eliminated through the development or design of the high-risk AI system, or the provision of adequate technical information.

4. The risk management measures referred to in paragraph 2, point (d), shall give due consideration to the effects and possible interaction resulting from the combined application of the requirements set out in this Section, with a view to minimising risks more effectively while achieving an appropriate balance in implementing the measures to fulfil those requirements.

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

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

(a) elimination or reduction of risks identified and evaluated pursuant to paragraph 2 in as far as technically feasible through adequate design and development of the high-risk AI system;

(b) where appropriate, implementation of adequate mitigation and control measures addressing risks that cannot be eliminated;

(c) provision of information required pursuant to Article 13 and, where appropriate, training to deployers.

With a view to eliminating or reducing risks related to the use of the high-risk AI system, due consideration shall be given to the technical knowledge, experience,

education, the training to be expected by the deployer, and the presumable context in which the system is intended to be used.

6. High-risk AI systems shall be tested for the purpose of identifying the most appropriate and targeted risk management measures. Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and that they are in compliance with the requirements set out in this Section.

7. Testing procedures may include testing in real-world conditions in accordance with Article 60.

8. The testing of high-risk AI systems shall be performed, as appropriate, at any time throughout the development process, and, in any event, prior to their being placed on the market or put into service. Testing shall be carried out against prior defined metrics and probabilistic thresholds that are appropriate to the intended purpose of the high-risk AI system.

9. When implementing the risk management system as provided for in paragraphs 1 to 7, providers shall give consideration to whether in view of its intended purpose the high-risk AI system is likely to have an adverse impact on persons under the age of 18 and, as appropriate, other vulnerable groups.

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

Article 10

Data and data governance

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

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

(a) the relevant design choices;

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

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

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

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

(f) examination in view of possible biases that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited under Union law, especially where data outputs influence inputs for future operations;

(g) appropriate measures to detect, prevent and mitigate possible biases identified according to point (f);

(h) the identification of relevant data gaps or shortcomings that prevent compliance with this Regulation, and how those gaps and shortcomings can be addressed.

3. Training, validation and testing data sets shall be relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used. Those characteristics of the data sets may be met at the level of individual data sets or at the level of a combination thereof.

4. Data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, contextual, behavioural or functional setting within which the high-risk AI system is intended to be used.

5. To the extent that it is strictly necessary for the purpose of ensuring bias detection and correction in relation to the high-risk AI systems in accordance with paragraph (2), points (f) and (g) of this Article, the providers of such systems may exceptionally process special categories of personal data, subject to appropriate safeguards for 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, all the following conditions must be met in order for such processing to occur:

(a) the bias detection and correction cannot be effectively fulfilled by processing other data, including synthetic or anonymised data;

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

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

(d)the special categories of personal data are not to be transmitted, transferred or otherwise accessed by other parties;

(e)the special categories of personal data are deleted once the bias has been corrected or the personal data has reached the end of its retention period, whichever comes first;

(f)the 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 biases, and why that objective could not be achieved by processing other data.

6. For the development of high-risk AI systems not using techniques involving the training of AI models, paragraphs 2 to 5 apply only to the testing data sets.

Article 11

Technical documentation

1. The technical documentation of a high-risk AI system shall be drawn up before that system is placed on the market or put into service and shall be kept up-to date.

The technical documentation shall be drawn up in such a way as to demonstrate that the high-risk AI system complies with the requirements set out in this Section and to provide national competent authorities and notified bodies with the necessary information in a clear and comprehensive form to assess the compliance of the AI system with those requirements. It shall contain, at a minimum, the elements set out in Annex IV. SMEs, including start-ups, may provide the elements of the technical documentation specified in Annex IV in a simplified manner. To that end, the Commission shall establish a simplified technical documentation form targeted at the needs of small and microenterprises. Where an SME, including a start-up, opts to provide the information required in Annex IV in a simplified manner, it shall use the form referred to in this paragraph. Notified bodies shall accept the form for the purposes of the conformity assessment.

2. Where a high-risk AI system related to a product covered by the Union harmonisation legislation listed in Section A of Annex I is placed on the market or put into service, a single set of technical documentation shall be drawn up containing all the information set out in paragraph 1, as well as the information required under those legal acts.

3. The Commission is empowered to adopt delegated acts in accordance with Article 97 in order to amend Annex IV, where necessary, to ensure that, in light of technical progress, the technical documentation provides all the information necessary to assess the compliance of the system with the requirements set out in this Section.

Article 12

Record-keeping

1. High-risk AI systems shall technically allow for the automatic recording of events (logs) over the lifetime of the system.

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

(a) identifying situations that may result in the high-risk AI system presenting a risk within the meaning of Article 79(1) or in a substantial modification;

(b) facilitating the post-market monitoring referred to in Article 72; and

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

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

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

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

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

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

Article 13

Transparency and provision of information to deployers

1. High-risk AI systems shall be designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable deployers to interpret a system's output and use it appropriately. An appropriate type and degree of transparency shall be ensured with a view to achieving compliance with the relevant obligations of the provider and deployer set out in Section 3.

2. High-risk AI systems shall be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to deployers.

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

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

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

(i) its intended purpose;

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

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

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

(v)when appropriate, its performance regarding specific persons or groups of persons on which the system is intended to be used;

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

(vii)where applicable, information to enable deployers to interpret the output of the high-risk AI system and use it appropriately;

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

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

(e)the computational and hardware resources needed, the expected lifetime of the high-risk AI system and any necessary maintenance and care measures, including their frequency, to ensure the proper functioning of that AI system, including as regards software updates;

(f)where relevant, a description of the mechanisms included within the high-risk AI system that allows deployers to properly collect, store and interpret the logs in accordance with Article 12.

Article 14

Human oversight

1. High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use.

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

3. The oversight measures shall be commensurate with the risks, level of autonomy and context of use of the high-risk AI system, and shall be ensured through either one or both of the following types of measures:

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

(b) measures identified by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate to be implemented by the deployer.

4. For the purpose of implementing paragraphs 1, 2 and 3, the high-risk AI system shall be provided to the deployer in such a way that natural persons to whom human oversight is assigned are enabled, as appropriate and proportionate:

(a) to properly understand the relevant capacities and limitations of the high-risk AI system and be able to duly monitor its operation, including in view of detecting and addressing anomalies, dysfunctions and unexpected performance;

(b) to remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system (automation bias), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons;

(c) to correctly interpret the high-risk AI system's output, taking into account, for example, the interpretation tools and methods available;

(d) to decide, in any particular situation, not to use the high-risk AI system or to otherwise disregard, override or reverse the output of the high-risk AI system;

(e) to intervene in the operation of the high-risk AI system or interrupt the system through a 'stop' button or a similar procedure that allows the system to come to a halt in a safe state.

5. For high-risk AI systems referred to in point 1(a) of Annex III, the measures referred to in paragraph 3 of this Article shall be such as to ensure that, in addition, no action or decision is taken by the deployer on the basis of the identification resulting from 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 a separate verification by at least two natural persons shall not apply to high-risk AI systems used for the purposes of law enforcement, migration, border control or asylum, where Union or national law considers the application of this requirement to be disproportionate.

Article 15

Accuracy, robustness and cybersecurity

1. High-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they perform consistently in those respects throughout their lifecycle.

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

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

4. High-risk AI systems shall be as resilient as possible regarding errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems. Technical and organisational measures shall be taken in this regard.

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

High-risk AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way as to eliminate or reduce as far as possible the risk of possibly biased outputs influencing input for future operations (feedback loops), and as to ensure that any such feedback loops are duly addressed with appropriate mitigation measures.

5. High-risk AI systems shall be resilient against attempts by unauthorised third parties to alter their use, outputs or performance by exploiting system vulnerabilities.

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

The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training data set (data poisoning), or pre-trained components used in training (model poisoning), inputs designed to cause the AI model to make a mistake (adversarial examples or model evasion), confidentiality attacks or model flaws.

SECTION 3

Obligations of providers and deployers of high-risk AI systems and other parties

Article 16

Obligations of providers of high-risk AI systems

Providers of high-risk AI systems shall:

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

(b) indicate on the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, as applicable, their name, registered trade name or registered trade mark, the address at which they can be contacted;

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

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

(e) when under their control, keep the logs automatically generated by their high-risk AI systems as referred to in Article 19;

(f) ensure that the high-risk AI system undergoes the relevant conformity assessment procedure as referred to in Article 43, prior to its being 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 that is not possible, on its packaging or its accompanying documentation, to indicate conformity 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 actions and provide information as required in Article 20;

(k) upon a reasoned request of a national competent authority, demonstrate the conformity 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 put a quality management system in place that ensures compliance with this Regulation. That system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions, and shall include at least the following aspects:

(a) a strategy for regulatory compliance, including compliance with conformity assessment procedures and procedures for the management of modifications to the high-risk AI system;

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

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

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

(e) technical specifications, including standards, to be applied and, where the relevant harmonised standards are not applied in full or do not cover all of 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) systems and procedures for data management, including data acquisition, data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purpose of the placing on the market or the putting into service of high-risk AI systems;

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

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

(i) procedures related to the reporting of a serious incident in accordance with Article 73;

(j) the handling of communication with national competent authorities, other relevant authorities, including those providing or supporting the access to data, notified bodies, other operators, customers or other interested parties;

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

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

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

2. The implementation of the aspects referred to in paragraph 1 shall be proportionate to the size of the provider's organisation. Providers shall, in any event, respect the degree of rigour and the 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 regarding 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 pursuant to that law.

4. For providers that are financial institutions subject to requirements regarding their internal governance, arrangements or processes under Union financial services law, the obligation to put in place a quality management system, with the exception of paragraph 1, points (g), (h) and (i) of this Article, shall be deemed to be fulfilled by

complying with the rules on internal governance arrangements or processes pursuant to the relevant Union financial services law. To that end, any harmonised standards referred to in Article 40 shall be taken into account.

Article 18

Documentation keeping

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

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

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

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

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

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

2. Each Member State shall determine conditions under which the documentation referred to in paragraph 1 remains at the disposal of the national competent authorities for the period indicated in that paragraph for the cases when a provider or its authorised representative established on its territory goes bankrupt or ceases its activity prior to the end of that period.

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

Article 19

Automatically generated logs

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

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

Article 20

Corrective actions and duty of information

1. Providers of high-risk AI systems which 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 conformity with this Regulation shall immediately take the necessary corrective actions to bring that system into conformity, to withdraw it, to disable it, or to recall it, as appropriate. They shall inform the distributors of the high-risk AI system concerned and, where applicable, the deployers, the authorised representative and importers accordingly.

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

Article 21

Cooperation with competent authorities

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

2. Upon a reasoned request by a competent authority, providers shall also give the requesting competent authority, as applicable, access to the automatically generated logs of the high-risk AI system referred to in Article 12(1), to the extent such logs 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

Authorised representatives of providers of high-risk AI systems

1. Prior to making their high-risk AI systems available on the Union market, providers established in third countries shall, by written mandate, appoint an authorised representative which is established in the Union.

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

3. The authorised representative shall perform the tasks specified in the mandate received from the provider. It shall provide a copy of the mandate to the market surveillance authorities upon request, in one of the official languages of the institutions of the Union, as indicated by the competent authority. For the purposes of this Regulation, the mandate shall empower 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 an appropriate conformity assessment procedure has been carried out by the provider;

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

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

(d) cooperate with competent authorities, upon a reasoned request, in any action the latter take in relation to the high-risk AI system, in particular to reduce and mitigate the risks posed by the high-risk AI system;

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

The mandate shall empower the authorised representative to be addressed, in addition to or instead of the provider, by the competent authorities, on all issues related to ensuring compliance with this Regulation.

4. The authorised representative shall terminate the mandate if it considers or has reason to consider the provider to be acting contrary to its obligations pursuant to this Regulation. In such a case, it shall immediately inform the relevant market surveillance authority, as well as, where applicable, the relevant notified body, about the termination of the mandate and the reasons therefor.

Article 23

Obligations of importers

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

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

(b) the provider 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 instructions for use;

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

2. Where an importer has sufficient reason to consider that a high-risk AI system is not in conformity with this Regulation, or is falsified, or accompanied by falsified documentation, it shall not place the system on the market until it has been brought into conformity. 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, the authorised representative and the market surveillance authorities to that effect.

3. Importers shall indicate their name, registered trade name or registered trade mark, and the address at which they can be contacted on the high-risk AI system and on its packaging or its accompanying documentation, where applicable.

4. Importers shall ensure that, while a high-risk AI system is under their responsibility, storage or transport conditions, where applicable, do not jeopardise its compliance with the requirements set out in Section 2.

5. Importers shall keep, for a period of 10 years after the high-risk AI system has been placed on the market or put into service, a copy of the certificate issued by the notified body, where applicable, of the instructions for use, and of the EU declaration of conformity referred to in Article 47.

6. Importers shall provide the relevant competent authorities, upon a reasoned request, with all the necessary information and documentation, including that referred to in paragraph 5, to demonstrate the conformity of a high-risk AI system with the requirements set out in Section 2 in a language which can be easily understood by them. For this purpose, 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 action those authorities take in relation to a high-risk AI system placed on the market by the importers, in particular to reduce and mitigate the risks posed by it.

Article 24

Obligations of distributors

1. Before making a high-risk AI system available 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 instructions for use, and that the provider and the importer of that system, as applicable, have complied with their respective obligations as laid down in Article 16, points (b) and (c) and Article 23(3).

2. Where a distributor considers or has reason to consider, on the basis of the information in its possession, that a high-risk AI system is not in conformity with the requirements set out in Section 2, it shall not make the high-risk AI system available on the market until the system has been brought into conformity with those requirements. Furthermore, where the high-risk AI system presents a risk within the meaning of Article 79(1), the distributor shall inform the provider or the importer of the system, as applicable, to that effect.

3. Distributors shall ensure that, while a high-risk AI system is under their responsibility, storage or transport conditions, where applicable, do not jeopardise the compliance of the system with the requirements set out in Section 2.

4. A distributor that considers or has reason to consider, on the basis of the information in its possession, a high-risk AI system which it has made available on the market not to be in conformity with the requirements set out in Section 2, shall take the corrective actions necessary to bring that system into conformity with those requirements, to withdraw it or recall it, or shall ensure that the provider, the importer or any relevant operator, as appropriate, takes those corrective actions. Where the high-risk AI system presents a risk within the meaning of Article 79(1), the distributor shall immediately inform the provider or importer of the system and the authorities competent for the high-risk AI system concerned, giving details, in particular, of the non-compliance and of any corrective actions taken.

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

6. Distributors shall cooperate with the relevant competent authorities in any action those authorities take in relation to a high-risk AI system made available on the market by the distributors, in particular to reduce or mitigate the risk posed by it.

Article 25

Responsibilities along the AI value chain

1. Any distributor, importer, deployer or other third-party shall be considered to be a provider of a high-risk AI system for the purposes of this Regulation and shall be

subject to the obligations of the provider under Article 16, in any of the following circumstances:

(a) they put their name or trademark on a high-risk AI system already placed on the market or put into service, without prejudice to contractual arrangements stipulating that the obligations are otherwise allocated;

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

(c) they modify the intended purpose of an AI system, including a general-purpose AI system, which has not been classified as high-risk and has already been placed on the market or put into service in such a way 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 occur, the provider that initially placed the AI system on the market or put it into service shall no longer be considered to be a provider of that specific AI system for the purposes of this Regulation. That initial provider shall closely cooperate with new providers and shall make available the necessary information and provide the reasonably expected technical access and other assistance that are required for the fulfilment of the obligations set out in this Regulation, in particular regarding the compliance with the conformity assessment of high-risk AI systems. This paragraph shall not apply in cases where the initial provider has clearly specified that its AI system is not to be changed into a high-risk AI system and therefore does not fall under the obligation to hand over the documentation.

3. In the case of high-risk AI systems that are safety components of products covered by the Union harmonisation legislation listed in Section A of Annex I, the product manufacturer shall be considered to be the provider of the high-risk AI system, and shall be subject to the obligations under Article 16 under either of the following circumstances:

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

(b) the high-risk AI system is put into service under the name or trademark of the product manufacturer after the product has been placed on the market.

4. The provider of a high-risk AI system and the third party that supplies an AI system, tools, services, components, or processes that are used or integrated in a high-risk AI system shall, by written agreement, specify the necessary information, capabilities, technical access and other assistance based on the generally acknowledged state of the art, in order 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

making accessible to the public 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 model terms for contracts between providers of high-risk AI systems and third parties that supply tools, services, components or processes that are used for or integrated into high-risk AI systems. When developing those voluntary model terms, the AI Office shall take into account possible contractual requirements applicable in specific sectors or business cases. The voluntary model terms shall be published and be available free of charge in an easily usable electronic format.

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

Article 26

Obligations of deployers of high-risk AI systems

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

2. Deployers shall assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support.

3. The obligations set out in paragraphs 1 and 2, are without prejudice to other deployer obligations under Union or national law and to the deployer's freedom to organise its own resources and activities for the purpose of implementing the human oversight measures indicated by the provider.

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

5. Deployers shall monitor the operation of the high-risk AI system on the basis of the instructions for use and, where relevant, inform providers in accordance with Article 72. Where deployers have reason to consider that the use of the high-risk AI system in accordance with the instructions may result in that AI system presenting a risk within the meaning of Article 79(1), they shall, without undue delay, inform the provider or distributor and the relevant market surveillance authority, and shall suspend the use of that system. Where deployers have identified a serious incident, they shall also immediately inform first the provider, and then the importer or distributor and the relevant market surveillance authorities of that incident. If the deployer is not able to reach the provider, Article 73 shall apply *mutatis mutandis*. This obligation shall not

cover sensitive operational data of deployers of AI systems which are law enforcement authorities.

For deployers that are financial institutions subject to requirements regarding their internal governance, arrangements or processes under Union financial services law, the monitoring obligation set out in the first subparagraph shall be deemed to be fulfilled by complying with the rules on internal governance arrangements, processes and mechanisms pursuant to the relevant financial service law.

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

Deployers that are financial institutions subject to requirements regarding their internal governance, arrangements or processes under Union financial services law shall maintain the logs as part of the documentation kept pursuant to the relevant Union financial service law.

7. Before putting into service or using a high-risk AI system at the workplace, deployers who are employers shall inform workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system. This information shall be provided, where applicable, in accordance with the rules and procedures laid down in Union and national law and practice on information of workers and their representatives.

8. Deployers of high-risk AI systems that are public authorities, or Union institutions, bodies, offices or agencies shall comply with the registration obligations referred to in Article 49. When such deployers find that the high-risk AI system that they envisage using has not been registered in the EU database referred to in Article 71, they shall not use that system and shall inform the provider or the distributor.

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

10. Without prejudice to Directive (EU) 2016/680, in the framework of an investigation for the targeted search of a person suspected or convicted of having committed a criminal offence, the deployer of a high-risk AI system for post-remote biometric identification shall request an authorisation, *ex ante*, or without undue delay and no later than 48 hours, by a judicial authority or an administrative authority whose decision is binding and subject to judicial review, for the use of that system, except when it is used for the initial identification of a potential suspect based on objective and

verifiable facts directly linked to the offence. Each use shall be limited to what is strictly necessary for the investigation of a specific criminal offence.

If the authorisation requested pursuant to the first subparagraph is rejected, the use of the post-remote biometric identification system linked to that requested authorisation shall be stopped with immediate effect and the personal data linked to the use of the high-risk AI system for which the authorisation was requested shall be deleted.

In no case shall such high-risk AI system for post-remote biometric identification be used for law enforcement purposes in an untargeted way, without any link to a criminal offence, a criminal proceeding, a genuine and present or genuine and foreseeable threat of a criminal offence, or the search for a specific missing person. It shall be ensured that no decision that produces an adverse legal effect on a person may be taken by the law enforcement authorities based solely on the output of such post-remote biometric identification systems.

This paragraph 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 deployer, each use of such high-risk AI systems shall be documented in the relevant police file and shall be made available to the relevant market surveillance authority and the national data protection authority upon request, excluding the disclosure of sensitive operational data related to law enforcement. This subparagraph 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 and national data protection authorities on their use of post-remote biometric identification systems, excluding the disclosure of sensitive operational data related to law enforcement. The reports may be aggregated to cover more than one deployment.

Member States may introduce, in accordance with Union law, more restrictive laws on the use of post-remote biometric identification systems.

11. Without prejudice to Article 50 of this Regulation, deployers of high-risk AI systems referred to in Annex III that make decisions or assist in making decisions related to natural persons shall inform the natural persons that they are subject to the use of the high-risk AI system. For high-risk AI systems used for law enforcement purposes Article 13 of Directive (EU) 2016/680 shall apply.

12. Deployers shall cooperate with the relevant competent authorities in any action those authorities take in relation to the high-risk AI system in order to implement this Regulation.

Article 27

Fundamental rights impact assessment for high-risk AI systems

1. Prior to deploying a high-risk AI system referred to in Article 6(2), with the exception of high-risk AI systems intended to be used in the area listed in point 2 of Annex III, deployers that are bodies governed by public law, or are private entities providing public services, and deployers of high-risk AI systems referred to in points 5 (b) and (c) of Annex III, shall perform an assessment of the impact on fundamental rights that the use of such system may produce. For that purpose, deployers shall perform an assessment consisting of:

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

(b) a description of the period of time within which, and the frequency with which, each high-risk AI system is intended to be used;

(c) the categories of natural persons and groups likely to be affected by its use in the specific context;

(d) the specific risks of harm likely to have an impact on the categories of natural persons or groups of persons identified pursuant to point (c) of this paragraph, taking into account the information given by the provider pursuant to Article 13;

(e) a description of the implementation of human oversight measures, according to the instructions for use;

(f) the measures to be taken in the case of the materialisation of those risks, including the arrangements for internal governance and complaint mechanisms.

2. The obligation laid down in paragraph 1 applies to the first use of the high-risk AI system. The deployer may, in similar cases, rely on previously conducted fundamental rights impact assessments or existing impact assessments carried out by provider. If, during the use of the high-risk AI system, the deployer considers that any of the elements listed in paragraph 1 has changed or is no longer up to date, the deployer shall take the necessary steps to update the information.

3. Once the assessment referred to in paragraph 1 of this Article has been performed, the deployer shall notify the market surveillance authority of its results, submitting the filled-out template referred to in paragraph 5 of this Article as part of the notification. In the case referred to in Article 46(1), deployers may be exempt from that obligation to notify.

4. If any of the obligations laid down in this Article is already met through the data protection impact assessment conducted 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 template for a questionnaire, including through an automated tool, to facilitate deployers in complying with 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 designate or establish at least one notifying authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring. Those procedures shall be developed in cooperation between the notifying authorities of all Member States.

2. Member States may decide that the assessment and monitoring referred to in paragraph 1 is to be carried out by a national accreditation body within the meaning of, and in accordance with, Regulation (EC) No 765/2008.

3. Notifying authorities shall be established, organised and operated in such a way that no conflict of interest arises with conformity assessment bodies, and that the objectivity and impartiality of their activities are safeguarded.

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

5. Notifying authorities shall offer or provide neither any activities that conformity assessment bodies perform, nor any consultancy services on a commercial or competitive basis.

6. Notifying authorities shall safeguard the confidentiality of the information that they obtain, in accordance with Article 78.

7. Notifying authorities shall have an adequate number of competent personnel at their disposal for the proper performance of their tasks. Competent personnel shall have the necessary expertise, where applicable, for their function, in fields such as information technologies, AI and law, including the supervision of fundamental rights.

Article 29

Application of a conformity assessment body for notification

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

2. The application for notification shall be accompanied by a description of the conformity assessment activities, the conformity assessment module or modules and the types of AI systems for which the conformity assessment body claims to be competent, as well as by an accreditation certificate, where one exists, issued by a national accreditation body attesting that the conformity assessment body fulfils the requirements laid down in Article 31.

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

3. Where the conformity assessment body concerned cannot provide an accreditation certificate, it shall provide the notifying authority with all the documentary evidence necessary for the verification, recognition and regular monitoring of its compliance with the requirements laid down in Article 31.

4. For notified bodies which are designated under any other Union harmonisation legislation, all documents and certificates linked to those designations may be used to support their designation procedure under this Regulation, as appropriate. The notified body shall update the documentation referred to in paragraphs 2 and 3 of this Article whenever relevant changes occur, in order to enable the authority responsible for notified bodies to monitor and verify continuous compliance with all the requirements laid down in Article 31.

Article 30

Notification procedure

1. Notifying authorities may notify only conformity assessment bodies which have satisfied the requirements laid down in Article 31.

2. Notifying authorities shall notify the Commission and the other Member States, using the electronic notification tool 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 full details of the conformity assessment activities, the conformity assessment module or modules, the types of AI systems concerned, and the relevant attestation of competence. Where a notification is not based on an accreditation certificate as referred to in Article 29(2), the notifying authority shall provide the Commission and the other Member States with documentary evidence which attests to the competence of the conformity assessment body and to the arrangements in place to ensure that that body will be monitored regularly and will continue to satisfy the requirements laid down in Article 31.

4. The conformity assessment body concerned may perform the activities of a notified body only where no objections are raised by the Commission or the other Member States within two weeks of a notification by a notifying authority where it includes an accreditation certificate referred to in Article 29(2), or within two months of a notification by the notifying authority where it includes 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 view thereof, the Commission shall decide whether the authorisation is justified. The Commission shall address its decision to the Member State concerned and to the relevant conformity assessment body.

Article 31

Requirements relating to notified bodies

1. A notified body shall be established under the national law of a Member State and shall have legal personality.

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

3. The organisational structure, allocation of responsibilities, reporting lines and operation of notified bodies shall ensure confidence in their performance, and in the results of the conformity assessment activities that the notified bodies conduct.

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

5. Neither a conformity assessment body, its top-level management nor the personnel responsible for carrying out its conformity assessment tasks shall be directly involved in the design, development, marketing or use of high-risk AI systems, nor shall they represent the parties engaged in those activities. They shall not engage in any activity that might conflict with their independence of judgement or integrity in relation to conformity assessment activities for which they are notified. This shall, in particular, apply to consultancy services.

6. Notified bodies shall be organised and operated so as to safeguard the independence, objectivity and impartiality of their activities. Notified bodies shall document and

implement a structure and procedures to safeguard impartiality and to promote and apply the principles of impartiality throughout their organisation, personnel and assessment activities.

7. Notified bodies shall have documented procedures in place ensuring that their personnel, committees, subsidiaries, subcontractors and any associated body or personnel of external bodies maintain, in accordance with Article 78, the confidentiality of the information which comes into their possession during the performance of conformity assessment activities, except when its disclosure is required by law. The staff of notified bodies shall be bound to observe professional secrecy with regard to all information obtained in carrying out their tasks under this Regulation, except in relation to the notifying authorities of the Member State in which their activities are carried out.

8. Notified bodies shall have procedures for the performance of activities which take due account of the size of a provider, the sector in which it operates, its 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 in accordance with national law or that Member State is itself 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 requisite competence in the specific field, whether those tasks are carried out by notified bodies themselves or on their behalf and under their responsibility.

11. Notified bodies shall have sufficient internal competences to be able effectively to evaluate the tasks conducted by external parties on their behalf. The notified body shall have permanent availability of sufficient administrative, technical, legal and scientific personnel who possess experience and knowledge relating to the relevant types of AI systems, data and data computing, and relating to the requirements set out in Section 2.

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

Article 32

Presumption of conformity with requirements relating to notified bodies

Where a conformity assessment body demonstrates its conformity with the criteria laid down in the relevant harmonised standards or parts thereof, the references of which have been published in the *Official Journal of the European Union*, it shall be presumed

to comply with the requirements set out in Article 31 in so far as the applicable harmonised standards cover those requirements.

Article 33

Subsidiaries of notified bodies and subcontracting

1. Where a notified body subcontracts specific tasks connected with the conformity assessment or has recourse to a subsidiary, it shall ensure that the subcontractor or the subsidiary meets the requirements laid down in Article 31, and shall inform the notifying authority accordingly.

2. Notified bodies shall take full responsibility for the tasks performed by any subcontractors or subsidiaries.

3. Activities may be subcontracted or carried out by a subsidiary only with the agreement of the provider. Notified bodies shall make a list of their subsidiaries publicly available.

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

Article 34

Operational obligations of notified bodies

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

2. Notified bodies shall avoid unnecessary burdens for providers when performing their activities, and 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 in view of minimising administrative burdens and compliance costs for micro- and small enterprises within the meaning of Recommendation 2003/361/EC. The notified body shall, nevertheless, respect the degree of rigour and the level of protection required for the compliance of the high-risk AI system with the requirements of this Regulation.

3. Notified bodies shall make available and submit upon request all relevant documentation, including the providers' documentation, to the notifying authority referred to in Article 28 to allow that authority to conduct its assessment, designation, notification and monitoring activities, and to facilitate the assessment outlined in this Section.

Article 35

Identification numbers and lists of notified bodies

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

2. The Commission shall make publicly available the list of the 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 to 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 via the electronic notification tool 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 changes to the notification other than extensions of its scope, the procedures laid down in paragraphs (3) to (9) shall apply.

3. Where a notified body decides to cease its conformity assessment activities, it shall inform the notifying authority and the providers concerned as soon as possible and, in the case of a planned cessation, at least one year before ceasing its activities. The certificates of the notified body may remain valid for a period of nine months after cessation of the notified body's activities, on condition that another notified body has confirmed in writing that it will assume responsibilities for the high-risk AI systems covered by those certificates. The latter notified body shall complete a full assessment of the high-risk AI systems affected by the end of that nine-month-period before issuing new certificates for those systems. Where the notified body has ceased its activity, the notifying authority shall withdraw the designation.

4. Where a notifying authority has sufficient reason to consider that a notified body no longer meets the requirements laid down in Article 31, or that it is failing to fulfil its obligations, the notifying authority shall without delay investigate the matter with the utmost diligence. In that context, it shall inform the notified body concerned about the objections raised and give it the possibility to make its views known. If the notifying authority comes to the conclusion that the notified body no longer meets the requirements laid down in Article 31 or that it is failing to fulfil its obligations, it shall restrict, suspend or withdraw the designation as appropriate, depending on the seriousness of the failure to meet those requirements or fulfil those obligations. It shall immediately inform the Commission and the other Member States accordingly.

5. Where its designation has been suspended, restricted, or fully or partially withdrawn, the notified body shall inform the providers concerned within 10 days.

6. In the event of the restriction, suspension or withdrawal of a designation, the notifying authority shall take appropriate steps to ensure that the files of the notified body concerned are kept, and to make them available to notifying authorities in other Member States and to market surveillance authorities at their request.

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

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

(b) submit a report on its findings to the Commission and the other Member States within three months of having notified the changes to the designation;

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

(d) inform the Commission and the Member States about certificates the suspension or withdrawal of which it has required;

(e) provide the national competent authorities of the Member State in which the provider has its registered place of business with all relevant information about the certificates of which it has required the suspension or withdrawal; that authority shall take the appropriate measures, where necessary, to avoid a potential risk to health, safety or fundamental rights.

8. With the exception of certificates unduly issued, and where a designation has been suspended or restricted, the certificates shall remain valid in one of the following circumstances:

(a) the notifying authority has confirmed, within one month of the suspension or restriction, that there is no risk to health, safety or fundamental rights in relation to certificates affected by the suspension or restriction, and the notifying authority has outlined a timeline for actions to remedy the suspension or restriction; or

(b) the notifying authority has confirmed that no certificates relevant to the suspension will be issued, amended or re-issued during the course of the suspension or restriction, and states whether the notified body has the capability of continuing to monitor and remain responsible for existing certificates issued for the period of the suspension or restriction; in the event that the notifying authority determines that the notified body does not have the capability to support existing certificates issued, the provider of the system covered by the certificate shall confirm in writing to the national competent authorities of the Member State in which it has its registered place of business, within three months of the suspension or restriction, that another qualified notified body is temporarily assuming the functions of the notified body to monitor and remain responsible for the certificates during the period of suspension or restriction.

9. With the exception of certificates unduly issued, and where a designation has been withdrawn, the certificates shall remain valid for a period of nine months under the following circumstances:

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

(b) another notified body has confirmed in writing that it will assume immediate responsibility for those AI systems and completes its assessment within 12 months of the withdrawal of the designation.

In the circumstances referred to in the first subparagraph, the national competent authority of the Member State in which the provider of the system covered by the certificate has its place of business may extend the provisional validity of the certificates for additional periods of three months, which shall not exceed 12 months in total.

The national competent 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 thereof.

Article 37

Challenge to the competence of notified bodies

1. The Commission shall, where necessary, investigate all cases where there are reasons to doubt the competence of a notified body or the continued fulfilment by a notified body of the requirements laid down in Article 31 and of its applicable responsibilities.

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

3. The Commission shall ensure that all sensitive information obtained in the course of its investigations pursuant to this Article is treated confidentially in accordance with Article 78.

4. Where the Commission ascertains that a notified body does not meet or no longer meets 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 notification if necessary. Where the Member State fails to 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, with regard to high-risk AI systems, appropriate coordination and cooperation between notified bodies active in the conformity assessment procedures pursuant to this Regulation are put in place and properly operated in the form of a sectoral group of notified bodies.

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

3. The Commission shall provide for the exchange of knowledge and best practices 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 meet the requirements laid down in Article 31 or they ensure an equivalent level of compliance.

SECTION 5

Standards, conformity assessment, certificates, registration

Article 40

Harmonised standards and standardisation deliverables

1. High-risk AI systems or general-purpose AI models which are in conformity with harmonised standards or parts thereof the references of which have been published in the *Official Journal of the European Union* in accordance with Regulation (EU) No 1025/2012 shall be presumed to be in conformity with the requirements set out in Section 2 of this Chapter or, as applicable, with the obligations set out in of Chapter V, Sections 2 and 3, of this Regulation, to the extent that those standards cover those requirements or obligations.

2. In accordance with Article 10 of Regulation (EU) No 1025/2012, the Commission shall issue, without undue delay, standardisation requests covering all requirements set

out in Section 2 of this Chapter and, as applicable, standardisation requests covering obligations set out in Chapter V, Sections 2 and 3, of this Regulation. The standardisation request shall also ask for deliverables on reporting and documentation processes to improve AI systems' resource performance, such as reducing the high-risk AI system's consumption of energy and of other resources during its lifecycle, and on the energy-efficient development of general-purpose AI models. When preparing a standardisation request, the Commission shall consult the Board and relevant stakeholders, including the advisory forum.

When issuing a standardisation request to European standardisation organisations, the Commission shall specify that standards have to be clear, consistent, including with the standards developed in the various sectors for products covered by the existing Union harmonisation legislation listed in Annex I, and aiming to ensure that high-risk AI systems or general-purpose AI models placed on the market or put into service in the Union meet the relevant requirements or obligations laid down in this Regulation.

The Commission shall request the European standardisation organisations to provide evidence of their best efforts to fulfil the objectives referred to in the first and the second subparagraph of this paragraph in accordance with Article 24 of Regulation (EU) No 1025/2012.

3. The participants in the standardisation process shall seek to promote investment and innovation in AI, including through increasing legal certainty, as well as the competitiveness and growth of the Union market, to contribute to strengthening global cooperation on standardisation and taking into account existing international standards in the field of AI that are consistent with Union values, fundamental rights and interests, and to enhance multi-stakeholder governance ensuring a balanced representation of interests and the effective participation of all relevant stakeholders in accordance with Articles 5, 6, and 7 of Regulation (EU) No 1025/2012.

Article 41

Common specifications

1. The Commission may adopt, implementing acts establishing common specifications for the requirements set out in Section 2 of this Chapter or, as applicable, for the obligations set out in Sections 2 and 3 of Chapter V where the following conditions have been fulfilled:

(a) the Commission has requested, pursuant to Article 10(1) of Regulation (EU) No 1025/2012, one or more European standardisation organisations to draft a harmonised standard for the requirements set out in Section 2 of this Chapter, or, as applicable, for the obligations set out in Sections 2 and 3 of Chapter V, and:

(i) the request has not been accepted by any of the European standardisation organisations; or

(ii) the harmonised standards addressing that request are not delivered within the deadline set in accordance with Article 10(1) of Regulation (EU) No 1025/2012; or

(iii) the relevant harmonised standards insufficiently address fundamental rights concerns; or

(iv) the harmonised standards do not comply with the request; and

(b) no reference to harmonised standards covering the requirements referred to in Section 2 of this Chapter or, as applicable, the obligations referred to in Sections 2 and 3 of Chapter V has been published in the *Official Journal of the European Union* in accordance with Regulation (EU) No 1025/2012, and no such reference is expected to be published within a reasonable period.

When drafting the common specifications, the Commission shall consult the advisory 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 preparing a draft implementing act, the Commission shall inform the committee referred to in Article 22 of Regulation (EU) No 1025/2012 that it considers the conditions laid down in paragraph 1 of this Article to be fulfilled.

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

4. Where a harmonised standard is adopted by a European standardisation organisation and proposed to the Commission for the publication of its reference in the *Official Journal of the European Union*, the Commission shall assess the harmonised standard in accordance with Regulation (EU) No 1025/2012. When reference to a harmonised standard is published in the *Official Journal of the European Union*, the Commission shall repeal the implementing acts referred to in paragraph 1, or parts thereof which cover the same requirements set out in Section 2 of this Chapter or, as applicable, the same obligations set out in Sections 2 and 3 of Chapter V.

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 meet the requirements referred to in Section 2 of this Chapter or, as applicable, comply with the obligations set out in Sections 2 and 3 of Chapter V to a level at least equivalent thereto.

6. Where a Member State considers that a common specification does not entirely meet the requirements set out in Section 2 or, as applicable, comply with obligations set out in Sections 2 and 3 of Chapter V, it shall inform the Commission thereof with

a detailed explanation. The Commission shall assess that information and, if appropriate, amend the implementing act establishing the common specification concerned.

Article 42

Presumption of conformity with certain requirements

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

2. High-risk AI systems that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 and the references of which have been published in the *Official Journal of the European Union* shall be presumed to comply with the cybersecurity requirements set out in Article 15 of this Regulation in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements.

Article 43

Conformity assessment

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

(a) the internal control referred to in Annex VI; or

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

In demonstrating the compliance of a high-risk AI system with the requirements set out in Section 2, the provider shall follow the conformity assessment procedure set out in Annex VII where:

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

(b) the provider has not applied, or has applied only part of, the harmonised standard;

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

(d) one or more of the harmonised standards referred to in point (a) has been published with a restriction, and only on the part of the standard that was restricted.

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, immigration or asylum authorities or by Union institutions, bodies, offices or agencies, the market surveillance authority referred to in Article 74(8) or (9), as applicable, shall act as a notified body.

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

3. For high-risk AI systems covered by the Union harmonisation legislation listed in Section A of Annex I, the provider shall follow the relevant conformity assessment procedure as required under those legal acts. The requirements set out in Section 2 of this Chapter shall apply to those high-risk AI systems and shall be part of that assessment. Points 4.3., 4.4., 4.5. and the fifth paragraph of point 4.6 of Annex VII shall also apply.

For the purposes of that assessment, notified bodies which have been notified under those legal acts shall be entitled to control the conformity of the high-risk AI systems with the requirements set out in Section 2, provided that the compliance of those notified bodies with requirements laid down in Article 31(4), (5), (10) and (11) has been assessed in the context of the notification procedure under those legal acts.

Where a legal act listed in Section A of Annex I enables the product manufacturer to opt out from a third-party conformity assessment, provided that that manufacturer has applied all harmonised standards covering all the relevant requirements, that manufacturer may use that option only if it has also applied harmonised standards or, where applicable, common specifications referred to in Article 41, covering all 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 undergo a new conformity assessment procedure in the event of a substantial modification, regardless of whether the modified system is intended to be further distributed or continues to be used by the current deployer.

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

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

6. The Commission is empowered to adopt delegated acts in accordance with Article 97 in order 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 such 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 the risks to health and safety and protection of fundamental rights posed by such systems, as well as the availability of adequate capacities and resources among 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 in the Member State in which the notified body is established.

2. Certificates shall be valid for the period they indicate, which shall not exceed five years for AI systems covered by Annex I, and four years for AI systems covered by Annex III. At the request of the provider, the validity of a certificate may be extended for further periods, each not exceeding five years for AI systems covered by Annex I, and four years for AI systems covered by Annex III, based on a re-assessment in accordance with the applicable conformity assessment procedures. Any supplement to a certificate shall remain valid, provided that the certificate which it supplements is valid.

3. Where a notified body finds that an AI system no longer meets the requirements set out in Section 2, it shall, taking account of 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 action taken by the provider of the system within an appropriate deadline set by the notified body. The notified body shall give reasons for its decision.

An appeal procedure against decisions of the notified bodies, including on conformity certificates issued, shall be available.

Article 45

Information obligations of notified bodies

1. Notified bodies shall inform the notifying authority of the following:

(a) any Union technical documentation assessment certificates, any supplements to those certificates, and any quality management system approvals issued in accordance with the requirements of Annex VII;

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

(c) any circumstances affecting the scope of or conditions for notification;

(d) any request for information which they have received from market surveillance authorities regarding conformity assessment activities;

(e) on request, conformity assessment activities performed within the scope of their notification and any other activity performed, including cross-border activities and subcontracting.

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

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

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

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

4. Notified bodies shall safeguard the confidentiality of the information that they obtain, in accordance with Article 78.

Article 46

Derogation from conformity assessment procedure

1. By way of derogation from Article 43 and upon a duly justified request, any market surveillance authority may authorise the placing on the market or the putting into service of specific high-risk AI systems within the territory of the Member State concerned, for exceptional reasons of public security or the protection of life and health of persons, environmental protection or the protection of key industrial and infrastructural assets. That authorisation shall be for a limited period while the necessary conformity assessment procedures are being carried out, taking into account the exceptional reasons justifying the derogation. The completion of those procedures shall be undertaken without undue delay.

2. In a duly justified situation of urgency for exceptional reasons of public security or in the case of specific, substantial and imminent threat to the life or physical safety of natural persons, law-enforcement authorities or civil protection authorities may put a specific high-risk AI system into service 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 stopped with immediate effect and all the results and outputs of such use shall be immediately discarded.

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

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

5. Where, within 15 calendar days of receipt of the notification referred to in paragraph 3, objections are raised by a Member State against an authorisation issued by a market surveillance authority of another Member State, or where the Commission considers the authorisation to be contrary to Union law, or the conclusion of the Member States regarding the compliance of the system as referred to in paragraph 3 to be unfounded, the Commission shall, without delay, enter into consultations with the relevant Member State. The operators concerned shall be consulted and have the possibility to present their views. Having regard thereto, the Commission shall decide whether the authorisation is justified. The Commission shall address its decision to the Member State concerned and to the relevant operators.

6. Where the Commission considers the authorisation unjustified, it shall be withdrawn by the market surveillance authority of the Member State concerned.

7. For high-risk AI systems related to products covered by Union harmonisation legislation listed in Section A of Annex I, only the derogations from the conformity assessment established in that Union harmonisation legislation shall apply.

Article 47

EU declaration of conformity

1. The provider shall draw up a written machine readable, physical or electronically signed EU declaration of conformity for each high-risk AI system, and keep it at the disposal of the national competent authorities for 10 years after the high-risk AI system has been placed on the market or put into service. The EU declaration of conformity shall identify the high-risk AI system for which it has been drawn up. A copy of the EU

declaration of conformity shall be submitted to the relevant national competent authorities upon request.

2. The EU declaration of conformity shall state that the high-risk AI system concerned meets 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 national competent authorities of the Member States in which the high-risk AI system is placed on the market or made available.

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 in respect of all Union law applicable to the high-risk AI system. The declaration shall contain all the information required to identify the Union harmonisation legislation to which the declaration relates.

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

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

Article 48

CE marking

1. The CE marking shall be subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008.

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

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

4. Where applicable, the CE marking shall be followed by the identification number of the notified body responsible for the conformity assessment procedures set out in Article 43. The identification number of the notified body shall be affixed by the body itself or, under its instructions, by the provider or by the provider’s authorised representative. The identification number shall also be indicated in any promotional

material which mentions that the high-risk AI system fulfils the requirements for CE marking.

5. Where high-risk AI systems are subject to other Union law which also provides for the affixing of the CE marking, the CE marking shall indicate that the high-risk AI system also fulfil the requirements of that other law.

Article 49

Registration

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 referred to in point 2 of Annex III, the provider or, where applicable, the authorised representative shall register themselves and their system in the EU database referred to in Article 71.

2. Before placing on the market or putting into service an AI system for which the provider has concluded that it is not high-risk according to Article 6(3), that provider or, where applicable, the authorised representative shall register themselves and 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 listed in point 2 of Annex III, deployers that are public authorities, Union institutions, bodies, offices or agencies or persons acting on their behalf shall register themselves, select the system and register its use in the EU database referred to in Article 71.

4. For 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 in a secure non-public section of the EU database referred to in Article 71 and shall include only the following information, as applicable, referred to in:

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

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

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

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

Only the Commission and 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 point 2 of Annex III shall be registered at national level.

CHAPTER IV
TRANSPARENCY OBLIGATIONS FOR PROVIDERS AND DEPLOYERS OF CERTAIN AI SYSTEMS

Article 50

Transparency obligations for providers and deployers of 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, unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use. This obligation 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 those systems are available for the public to report 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 outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated. Providers shall ensure their technical solutions are effective, interoperable, robust and reliable as far as this is technically feasible, taking into account the specificities and limitations of various types of content, the costs of implementation and the generally acknowledged state of the art, as may be reflected in relevant technical standards. This obligation shall not apply to the extent the AI systems perform an assistive function for standard editing or do not substantially alter the input data provided by the deployer or the semantics thereof, or where authorised by law to detect, prevent, investigate or prosecute criminal offences.

3. Deployers of an emotion recognition system or a biometric categorisation system shall inform the natural persons exposed thereto of the operation of the system, and shall process the 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, which are permitted by law to detect, prevent or investigate criminal offences, subject to appropriate safeguards for the rights and freedoms of third parties, and in accordance with Union law.

4. Deployers of an AI system that generates or manipulates image, audio or video content constituting a deep fake, shall disclose that the content 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 offence. Where the content forms part of an evidently artistic, creative, satirical, fictional or analogous work or

programme, the transparency obligations set out in this paragraph are limited to disclosure of the existence of such generated or manipulated content in an appropriate manner that does not hamper the display or enjoyment of the work.

Deployers of an AI system that generates or manipulates text which is published with 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 undergone a process of human review or editorial control and where a natural or legal person holds editorial responsibility for the publication of the content.

5. The information referred to in paragraphs 1 to 4 shall be provided to the natural persons concerned in a clear and distinguishable manner at the latest at the time of the first interaction or exposure. The information shall conform to the 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 laid down in Union or national law for deployers of AI systems.

7. The AI Office shall encourage and facilitate the drawing up of codes of practice at Union level to facilitate the effective implementation of the obligations regarding the detection and labelling of artificially generated or manipulated content. The Commission may adopt implementing acts to approve those codes of practice in accordance with the procedure laid down in Article 56 (6). If it deems the code is not adequate, the Commission may adopt an implementing act specifying common rules for the implementation 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

Classification of general-purpose AI models as general-purpose AI models with systemic risk

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) it has high impact capabilities evaluated on the basis of appropriate technical tools and methodologies, including indicators and benchmarks;

(b) based on a decision of the Commission, *ex officio* or following a qualified alert from the scientific panel, it has capabilities or an impact equivalent to those set out in point (a) having regard to the criteria set out in Annex XIII.

2. A general-purpose AI model shall be presumed to have high impact capabilities pursuant to paragraph 1, point (a), when the cumulative amount of computation used for its training 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 listed in paragraphs 1 and 2 of this Article, as well as to supplement benchmarks and indicators in light of evolving technological developments, such as algorithmic improvements or increased hardware efficiency, when necessary, for these thresholds to reflect the state of the art.

Article 52

Procedure

1. Where a general-purpose AI model meets the condition referred to in Article 51(1), point (a), the relevant provider shall notify the Commission without delay and in any event within two weeks after that requirement is met or it becomes known that it will be met. That notification shall include the information necessary to demonstrate that the relevant requirement has been met. If the Commission becomes aware of a general-purpose AI model presenting systemic risks of which it 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 Article 51(1), point (a), may present, with its notification, sufficiently substantiated arguments to demonstrate that, exceptionally, although it meets that requirement, the general-purpose AI model does not present, due to its specific characteristics, systemic risks and therefore should 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 the relevant provider was not able to demonstrate that the general-purpose AI model does not present, due to its specific characteristics, systemic risks, it shall reject those arguments, and the general-purpose AI model shall be considered to be a general-purpose AI model with systemic risk.

4. The Commission may designate a general-purpose AI model as presenting systemic risks, *ex officio* or following a qualified alert from the scientific panel pursuant to Article 90(1), point (a), on the basis of criteria set out in Annex XIII.

The Commission is empowered to adopt delegated acts in accordance with Article 97 in order to amend Annex XIII by specifying and updating the criteria set out in that Annex.

5. Upon a reasoned request of a provider whose model has been designated as a general-purpose AI model with systemic risk pursuant to paragraph 4, the Commission shall take the request into account and may decide to reassess whether the general-purpose AI model can still be considered to present systemic risks on the basis of the criteria set out in Annex XIII. Such a request shall contain objective, detailed and new reasons that have arisen since the designation decision. Providers may request reassessment at the earliest six months after the designation decision. Where the Commission, following its reassessment, decides to maintain the designation as a general-purpose AI model with systemic risk, providers may request reassessment at the earliest six months after that decision.

6. The Commission shall ensure that a list of general-purpose AI models with systemic risk is published and shall keep that list up to date, 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.

SECTION 2

Obligations for providers of general-purpose AI models

Article 53

Obligations for providers of general-purpose AI models

1. Providers of general-purpose AI models shall:

(a) draw up and keep up-to-date the technical documentation of the model, including its training and testing process and the results of its evaluation, which shall contain, at a minimum, the information set out in Annex XI for the purpose of providing it, upon request, to the AI Office and the national competent authorities;

(b) draw up, keep up-to-date and make available information and documentation to providers of AI systems who intend 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, the information and documentation shall:

(i) enable providers of AI systems to have a good understanding of the capabilities and limitations of the general-purpose AI model and to comply with their obligations pursuant to this Regulation; and

(ii) contain, at a minimum, the elements set out in Annex XII;

(c) put in place a policy to comply with Union law on copyright and related rights, and in particular to identify and comply with, including through state-of-the-art technologies, a reservation of rights expressed pursuant to Article 4(3) of Directive (EU) 2019/790;

(d) draw up and make publicly available a sufficiently detailed summary about the content used for training of the general-purpose AI model, according to a template provided by the AI Office.

2. The obligations set out in paragraph 1, points (a) and (b), shall not apply to providers of AI models that are released under a free and open-source licence that allows for the access, usage, modification, and distribution of the model, and whose parameters, including the weights, the information on the model architecture, and the information on model usage, are made publicly available. This exception shall not apply to general-purpose AI models with systemic risks.

3. Providers of general-purpose AI models shall cooperate as necessary with the Commission and the national competent authorities in the exercise of their competences and powers pursuant to 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 the presumption of conformity to the extent that those standards cover those obligations. Providers of general-purpose AI models who do not adhere to an approved code of practice or do not comply with a European harmonised standard shall demonstrate alternative adequate means of compliance for assessment by the Commission.

5. For the purpose of facilitating compliance with Annex XI, in particular points 2 (d) and (e) thereof, the Commission is empowered to adopt delegated acts in accordance with Article 97 to detail measurement and calculation methodologies with a view to allowing for comparable and verifiable documentation.

6. The Commission is empowered to adopt delegated acts in accordance with Article 97(2) to amend Annexes XI and XII in light of evolving technological developments.

7. Any information or documentation obtained pursuant to this Article, including trade secrets, shall be treated in accordance with the confidentiality obligations set out in Article 78.

Article 54

Authorised representatives of providers of general-purpose AI models

1. Prior to placing a general-purpose AI model on the Union market, providers established in third countries shall, by written mandate, appoint an authorised representative which is established in the Union.

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

3. The authorised representative shall perform the tasks specified in the mandate received from the provider. It shall provide a copy of the mandate to the AI Office upon request, in one of the official languages of the institutions of the Union. For the purposes of this Regulation, the mandate shall empower the authorised representative to carry out the following tasks:

(a) verify that the technical documentation specified in Annex XI has been drawn up and all obligations referred to in Article 53 and, where applicable, Article 55 have been fulfilled by the provider;

(b) keep a copy of the technical documentation specified in Annex XI at the disposal of the AI Office and national competent authorities, for a period of 10 years after the general-purpose AI model has been placed on the market, and the contact details of the provider that appointed the authorised representative;

(c) provide the AI Office, upon a reasoned request, with all the information and documentation, including that referred to in point (b), necessary to demonstrate compliance with the obligations in this Chapter;

(d) cooperate with the AI Office and competent authorities, upon a reasoned request, in any action they take in relation to the general-purpose AI model, including when the model is integrated into AI systems placed on the market or put into service in the Union.

4. The mandate shall empower the authorised representative to be addressed, in addition to or instead of the provider, by the AI Office or the competent authorities, on all issues related to ensuring compliance with this Regulation.

5. The authorised representative shall terminate the mandate if it considers or has reason to consider the provider to be acting contrary to its obligations pursuant to this Regulation. In such a case, it shall also immediately inform the AI Office about 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 released under a free and open-source licence that allows for the access, usage, modification, and distribution of the model, and whose parameters, including the weights, the information on the model architecture, and the information on model usage, are made publicly available, unless the 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 shall:

(a) perform model evaluation in accordance with standardised protocols and tools reflecting the state of the art, including conducting and documenting adversarial testing of the model with a view to identifying and mitigating systemic risks;

(b) assess and mitigate possible systemic risks at Union level, including their sources, that may stem from the development, the placing on the market, or the use of general-purpose AI models with systemic risk;

(c) keep track of, document, and report, without undue delay, to the AI Office and, as appropriate, to national competent authorities, relevant information about serious incidents and possible corrective measures to address them;

(d) ensure an adequate level of cybersecurity protection 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 the presumption of conformity to the extent that those standards cover those obligations. Providers of general-purpose AI models with systemic risks who do not adhere to an approved code of practice or do not comply with a European harmonised standard shall demonstrate alternative adequate means of compliance for assessment by the Commission.

3. Any information or documentation obtained pursuant to this Article, including trade secrets, shall be treated in accordance with the confidentiality obligations set out in Article 78.

SECTION 4

Codes of practice

Article 56

Codes of practice

1. The AI Office shall encourage and facilitate the drawing up of codes of practice at Union level in order to contribute to the proper application of this Regulation, taking into account international approaches.

2. The AI Office and the Board shall aim to ensure that the codes of practice cover at least the obligations provided for in Articles 53 and 55, including the following issues:

(a) the means to ensure that the information referred to in Article 53(1), points (a) and (b), is kept up to date in light of market and technological developments;

(b) the adequate level of detail for the summary about the content used for training;

(c) the identification of the type and nature of the systemic risks at Union level, including their sources, where appropriate;

(d) the measures, procedures and modalities for the assessment and management of the systemic risks at Union level, including the documentation thereof, which shall be proportionate to the risks, take into consideration their severity and probability and take into account the specific challenges of tackling those risks in light of the possible ways in which such risks may emerge 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 drawing-up of codes of practice. Civil society organisations, industry, academia and other relevant stakeholders, such as downstream providers and independent experts, may support the process.

4. The AI Office and the Board shall aim to ensure that the codes of practice clearly set out their specific objectives and contain commitments or measures, including key performance indicators as appropriate, to ensure the achievement of those objectives, and that they take due account of the needs and interests of all interested parties, including affected persons, at Union level.

5. The AI Office shall aim to ensure that participants to the codes of practice report regularly to the AI Office on the implementation of the commitments and the measures taken and their outcomes, including as measured against the key performance indicators as appropriate. Key performance indicators and reporting commitments shall reflect differences in size and capacity between various participants.

6. The AI Office and the 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 Board shall assess whether the codes of practice cover the obligations provided for 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 way of an implementing act, approve a code of practice and give it a 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 practice. For providers of general-purpose AI models not presenting systemic risks this adherence may be limited to the obligations provided for in Article 53, unless they declare explicitly their interest to join the full code.

8. The AI Office shall, as appropriate, also encourage and facilitate the review and adaptation of the codes of practice, in particular in light of emerging standards. The AI Office shall assist in the assessment of available standards.

9. Codes of practice shall be ready at the latest by 2 May 2025. The AI Office shall take the necessary steps, including inviting providers pursuant to paragraph 7.

If, by 2 August 2025, a code of practice cannot be finalised, or if the AI Office deems it is not adequate following its assessment under paragraph 6 of this Article, the Commission may provide, by means of implementing acts, common rules for the implementation of the obligations provided for in Articles 53 and 55, including the issues 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 IN SUPPORT OF INNOVATION

Article 57

AI regulatory sandboxes

1. Member States shall ensure that their competent authorities establish at least one AI regulatory sandbox at national level, which shall be operational by 2 August 2026. That 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 regulatory sandboxes.

The obligation under the first subparagraph may also be fulfilled by participating in an existing sandbox in so far as that participation provides an equivalent level of national coverage for the participating Member States.

2. Additional AI regulatory sandboxes at regional or local level, or established jointly with the competent authorities of other Member States may also be established.

3. The European Data Protection Supervisor may also establish an AI regulatory sandbox for Union institutions, bodies, offices and agencies, and may exercise the roles and the tasks of national competent authorities in accordance with 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 effectively and in a timely manner. Where appropriate, national competent authorities shall cooperate with other relevant authorities, and may allow for the involvement of other actors within the AI ecosystem. This Article shall not affect other regulatory sandboxes established under Union or national law. Member States shall ensure an appropriate level of cooperation between the authorities supervising those other sandboxes and the national competent authorities.

5. AI regulatory sandboxes established under paragraph 1 shall provide for a controlled environment that fosters innovation and facilitates the development, training, testing and validation of innovative AI systems for a limited time before their being placed on the market or put into service pursuant to a specific sandbox plan agreed between the providers or prospective providers and the competent authority. Such sandboxes may include testing in real world conditions supervised therein.

6. Competent authorities shall provide, as appropriate, guidance, supervision and support within the AI regulatory sandbox with a view to identifying risks, in particular to fundamental rights, health and safety, testing, mitigation measures, and their effectiveness in relation to the obligations and requirements of this Regulation and, where relevant, other Union and national law supervised within the sandbox.

7. Competent authorities shall provide providers and prospective providers participating in the AI regulatory sandbox with guidance on regulatory expectations and how to fulfil the requirements and obligations set out in this Regulation.

Upon request of the provider or prospective provider of the AI system, the competent authority shall provide a written proof 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 such documentation to demonstrate their compliance with this Regulation through the conformity assessment process or relevant market surveillance activities. In this regard, the exit reports and the written proof provided by the national competent authority shall be taken positively into account by market surveillance authorities and notified bodies, with a view to accelerating conformity assessment procedures to a reasonable extent.

8. Subject to the confidentiality provisions in Article 78, and with the agreement of the provider or prospective provider, the Commission and the Board shall be authorised to access the exit reports and shall take them into account, as appropriate, when exercising their tasks under this Regulation. If both the provider or prospective provider and the national competent authority explicitly agree, the exit report may be made publicly available through the single information platform referred to in this Article.

9. The establishment of AI regulatory sandboxes shall aim to contribute to the following objectives:

(a) improving legal certainty to achieve regulatory compliance with this Regulation or, where relevant, other applicable Union and national law;

(b) supporting the sharing of best practices through cooperation with the authorities involved in the AI regulatory sandbox;

(c) fostering innovation and competitiveness and facilitating the development of an AI ecosystem;

(d) contributing to evidence-based regulatory learning;

(e) facilitating and accelerating 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 the innovative AI systems involve the processing of personal data or otherwise fall under the supervisory remit of other national authorities or competent authorities providing or supporting access to data, the national data protection authorities and those other national or competent authorities are associated with the operation of the AI regulatory sandbox and involved in the supervision of those aspects to the extent of their respective tasks and powers.

11. The AI regulatory sandboxes shall not affect the supervisory or corrective powers of the competent authorities supervising the sandboxes, including at regional or local level. Any significant risks to health and safety and fundamental rights identified during the development and testing of such AI systems shall result in an adequate mitigation. National competent authorities shall have the power to temporarily or permanently suspend the testing process, or the participation in the sandbox if no effective mitigation is possible, and shall inform the AI Office of such decision. National competent authorities shall exercise their supervisory powers within the limits of the relevant law, using their discretionary powers when implementing legal provisions in respect of a specific AI regulatory sandbox project, with the objective of supporting innovation in AI in the Union.

12. Providers and prospective providers participating in the AI regulatory sandbox shall remain liable under applicable Union and national liability law for any damage inflicted on third parties as a result of the experimentation taking place in the sandbox. However, provided that the prospective providers observe the specific plan and the terms and conditions for their participation and follow in good faith the guidance given by the national competent authority, no administrative fines shall be imposed by the authorities for infringements of this Regulation. Where other competent authorities responsible for other Union and national law were actively involved in the supervision of the AI system in the sandbox and provided guidance for compliance, no administrative fines shall be imposed regarding that law.

13. The AI regulatory sandboxes shall be designed and implemented in such a way that, where relevant, they facilitate cross-border cooperation between national competent authorities.

14. National competent authorities shall coordinate their activities and cooperate within the framework of the Board.

15. National competent authorities shall inform the AI Office and the Board of the establishment of a sandbox, and may ask them for support and guidance. The AI Office shall make publicly available a list of planned and existing sandboxes and keep it up to date in order to encourage more interaction in the AI regulatory sandboxes and cross-border cooperation.

16. National competent authorities shall submit annual reports to the AI Office and to the Board, from one year after the establishment of the AI regulatory sandbox and every year thereafter until its termination, and a final report. Those reports shall provide information on the progress and results of the implementation of those sandboxes, including best practices, incidents, lessons learnt and recommendations on their setup and, where relevant, on the application and possible revision of this Regulation, including its delegated and implementing acts, and on the application of other Union law supervised by the competent authorities within the sandbox. The national competent authorities shall make those annual reports or abstracts thereof available to the public, online. The Commission shall, where appropriate, take the annual reports into account when exercising its tasks under this Regulation.

17. The Commission shall develop a single and dedicated interface containing all relevant information related to AI regulatory sandboxes to allow stakeholders to interact with AI regulatory sandboxes and to raise enquiries with competent authorities, and to seek non-binding guidance on the conformity of innovative products, services, business models embedding AI technologies, in accordance with Article 62(1), point (c). The Commission shall proactively coordinate with national competent authorities, where relevant.

Article 58

Detailed arrangements for, and functioning of, AI regulatory sandboxes

1. In order to avoid fragmentation across the Union, the Commission shall adopt implementing acts specifying the detailed arrangements for the establishment, development, implementation, operation and supervision of the AI regulatory sandboxes. The implementing acts shall include common principles on the following issues:

(a) eligibility and selection criteria for participation in the AI regulatory sandbox;

(b)procedures for the application, participation, monitoring, exiting from and termination of the AI regulatory sandbox, including the sandbox plan and the exit report;

(c) the terms and conditions applicable to the 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 regulatory sandboxes are open to any applying provider or prospective provider of an AI system who fulfils eligibility and selection criteria, which shall be transparent and fair, and that national competent authorities inform applicants of their decision within three months of the application;

(b)that AI regulatory sandboxes allow broad and equal access and keep up with demand for participation; providers and prospective providers may also submit applications in partnerships with deployers and other relevant third parties;

(c)that the detailed arrangements for, and conditions concerning AI regulatory sandboxes support, to the best extent possible, flexibility for national competent authorities to establish and operate their AI regulatory sandboxes;

(d)that access to the AI regulatory sandboxes is free of charge for SMEs, including start-ups, without prejudice to exceptional costs that national competent authorities may recover in a fair and proportionate manner;

(e)that they facilitate providers and prospective providers, by means of the learning outcomes of the AI regulatory sandboxes, in complying with conformity assessment obligations under this Regulation and the voluntary application of the codes of conduct referred to in Article 95;

(f)that AI regulatory sandboxes facilitate the involvement of other relevant actors within the AI ecosystem, such as notified bodies and standardisation organisations, SMEs, including start-ups, enterprises, innovators, testing and experimentation facilities, research and experimentation labs and European Digital Innovation Hubs, centres of excellence, individual researchers, in order to allow and facilitate cooperation with the public and private sectors;

(g)that procedures, processes and administrative requirements for application, selection, participation and exiting the AI regulatory 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 regulatory sandbox established by a Member State, or by the European Data Protection Supervisor is mutually and uniformly recognised and carries the same legal effects across the Union;

(h)that participation in the AI regulatory sandbox is limited to a period that is appropriate to the complexity and scale of the project and that may be extended by the national competent authority;

(i)that AI regulatory sandboxes facilitate the development of tools and infrastructure for testing, benchmarking, assessing and explaining dimensions of AI systems relevant for regulatory learning, such as accuracy, robustness and cybersecurity, as well as measures to mitigate risks to fundamental rights and society at large.

3. Prospective providers in the AI regulatory sandboxes, in particular SMEs and start-ups, shall be directed, where relevant, to pre-deployment services such as guidance on the implementation of this Regulation, to other value-adding services such as help with standardisation documents and certification, testing and experimentation facilities, European Digital Innovation Hubs and centres of excellence.

4. Where national competent authorities consider authorising testing in real world conditions supervised within the framework of an AI regulatory sandbox to be established under this Article, they shall specifically agree the terms and conditions of such testing and, in particular, the appropriate safeguards with the participants, with a view to protecting fundamental rights, health and safety. Where appropriate, they shall cooperate with other national competent authorities with a view to ensuring consistent practices across the Union.

Article 59

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

1. In the AI regulatory sandbox, personal data lawfully collected for other purposes may be processed solely for the purpose of developing, training and testing certain AI systems in the sandbox when all of the following conditions are met:

(a)AI systems shall be developed for safeguarding substantial public interest by a public authority or another natural or legal person and in one or more of the following areas:

(i)public safety and public health, including disease detection, diagnosis prevention, control and treatment and improvement of health care systems;

(ii)a high level of protection and improvement of the quality of the environment, protection of biodiversity, protection against pollution, green transition measures, climate change mitigation and adaptation measures;

(iii) energy sustainability;

(iv)safety and resilience of transport systems and mobility, critical infrastructure and networks;

(v) efficiency and quality of public administration and public services;

(b) the data processed are necessary for complying with one or more of the requirements referred to in Chapter III, Section 2 where those requirements cannot effectively be fulfilled by processing anonymised, synthetic or other non-personal data;

(c) there are effective monitoring mechanisms to identify if any high risks to the rights and freedoms of the data subjects, as referred to in Article 35 of Regulation (EU) 2016/679 and in Article 39 of Regulation (EU) 2018/1725, may arise during the sandbox experimentation, as well as response mechanisms to promptly mitigate those risks and, where necessary, stop the processing;

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

(e) providers can further share the originally collected data only in accordance with Union data protection law; any personal data created in the sandbox cannot be shared outside the sandbox;

(f) any processing of personal data in the context of the sandbox neither leads to measures or decisions affecting the data subjects nor does it affect the application of their rights laid down in Union law on the protection of personal data;

(g) any personal data processed in the context of the sandbox are protected by means of appropriate technical and organisational measures and deleted once the participation in the sandbox has terminated or the personal data has reached the end of its retention period;

(h) the logs of the processing of personal data in the context of the sandbox are kept for the duration of the participation in the sandbox, unless provided otherwise by Union or national law;

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

(j) a short summary of the AI project developed in the sandbox, its objectives and expected results is published on the website of the competent authorities; this obligation shall not cover sensitive operational data in relation to the activities of law enforcement, border control, immigration or asylum authorities.

2. 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, under the control and responsibility of law enforcement authorities, the processing of personal data in AI regulatory sandboxes shall be based on a specific Union or national law and subject to the same cumulative conditions as referred to in paragraph 1.

3. Paragraph 1 is without prejudice to Union or national law which excludes processing of personal data for other purposes than those explicitly mentioned in that law, as well as to Union or national law laying down the basis for the processing of

personal data which is necessary for the purpose of developing, testing or training of innovative AI systems or any other legal basis, in compliance with Union law on the protection of personal data.

Article 60

Testing of high-risk AI systems in real world conditions outside AI regulatory sandboxes

1. Testing of high-risk AI systems in real world conditions outside AI regulatory sandboxes may be conducted by providers or prospective providers of high-risk AI systems listed in Annex III, in accordance with this Article and the real-world testing plan referred to in this Article, without prejudice to the prohibitions under Article 5.

The Commission shall, by means of implementing acts, specify the detailed elements of the real-world testing plan. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

This paragraph shall be without prejudice to Union or national law on the testing in real world conditions of high-risk AI systems related to products covered by Union harmonisation legislation listed in Annex I.

2. Providers or prospective providers may conduct testing of high-risk AI systems referred to in Annex III in real world conditions at any time before the placing on the market or the putting into service of the AI system on their own or in partnership with one or more deployers or prospective deployers.

3. The testing of high-risk AI systems in real world conditions under this Article shall be without prejudice to any ethical review that is required by Union or national law.

4. Providers or prospective providers may conduct the testing in real world conditions only where all of the following conditions are met:

(a) the provider or prospective provider has drawn up a real-world testing plan and submitted it to the market surveillance authority in the Member State where the testing in real world conditions is to be conducted;

(b) the market surveillance authority in the Member State where the testing in real world conditions is to be conducted has approved the testing in real world conditions and the real-world testing plan; where the market surveillance authority has not provided an answer within 30 days, the testing in real world conditions and the real-world testing plan shall be understood to have been approved; where national law does not provide for a tacit approval, the testing in real world conditions shall remain subject to an authorisation;

(c) the provider or prospective provider, with the exception of providers or prospective providers 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, and high-risk AI systems

referred to in point 2 of Annex III has registered the testing in real world conditions in accordance with Article 71(4) with a Union-wide unique single identification number and with the information specified in Annex IX; the provider or prospective provider 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, has registered the testing in real-world conditions in the secure non-public section of the EU database according to Article 49(4), point (d), with a Union-wide unique single identification number and with the information specified therein; the provider or prospective provider of high-risk AI systems referred to in point 2 of Annex III has registered the testing in real-world conditions in accordance with Article 49(5);

(d) the provider or prospective provider conducting the testing in real world 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 purpose of the testing in real world conditions shall be transferred to third countries only provided that appropriate and applicable safeguards under Union law are implemented;

(f) the testing in real world conditions does not last longer than necessary to achieve its objectives and in any case not longer than six months, which may be extended for an additional period of six months, subject to prior notification by the provider or prospective provider to the market surveillance authority, accompanied by an explanation of the need for such an extension;

(g) the subjects of the testing in real world conditions who are persons belonging to vulnerable groups due to their age or disability, are appropriately protected;

(h) where a provider or prospective provider organises the testing in real world conditions in cooperation with one or more deployers or prospective deployers, the latter have been informed of all aspects of the testing that are relevant to their decision to participate, and given the relevant instructions for use of the AI system referred to in Article 13; the provider or prospective provider and the deployer or prospective deployer shall conclude an agreement specifying their roles and responsibilities with a view to ensuring compliance with the provisions for testing in real world conditions under this Regulation and under other applicable Union and national law;

(i) the subjects of the testing in real world conditions have given informed consent in accordance with Article 61, or in the case of law enforcement, where the seeking of informed consent would prevent the AI system from being tested, the testing itself and the outcome of the testing in the real world conditions shall not have any negative effect on the subjects, and their personal data shall be deleted after the test is performed;

(j) the testing in real world conditions is effectively overseen by the provider or prospective provider, as well as by deployers or prospective deployers through persons who are suitably qualified in the relevant field and have the necessary capacity, training and authority to perform their tasks;

(k) the predictions, recommendations or decisions of the AI system can be effectively reversed and disregarded.

5. Any subjects of the testing in real world conditions, or their legally designated representative, as appropriate, may, without any resulting detriment and without having to provide any justification, withdraw from the testing at any time by revoking their informed consent and may request the immediate and permanent deletion of their personal data. The withdrawal of the informed consent shall not affect the activities already carried out.

6. In accordance with Article 75, Member States shall confer on their market surveillance authorities the powers of requiring providers and prospective providers to provide information, of carrying out unannounced remote or on-site inspections, and of performing checks on the conduct of the testing in real world conditions and the related high-risk AI systems. Market surveillance authorities shall use those powers to ensure the safe development of testing in real world conditions.

7. Any serious incident identified in the course of the testing in real world conditions shall be reported to the national market surveillance authority in accordance with Article 73. The provider or prospective provider shall adopt immediate mitigation measures or, failing that, shall suspend the testing in real world conditions until such mitigation takes place, or otherwise terminate it. The provider or prospective provider shall establish a procedure for the prompt recall of the AI system upon such termination of the testing in real world conditions.

8. Providers or prospective providers shall notify the national market surveillance authority in the Member State where the testing in real world conditions is to be conducted of the suspension or termination of the testing in real world conditions and of the final outcomes.

9. The provider or prospective provider shall be liable under applicable Union and national liability law for any damage caused in the course of their testing in real world conditions.

Article 61

Informed consent to participate in testing in real world conditions outside AI regulatory sandboxes

1. For the purpose of testing in real world conditions under Article 60, freely-given informed consent shall be obtained from the subjects of testing prior to their participation in such testing and after their having been duly informed with concise, clear, relevant, and understandable information regarding:

(a)the nature and objectives of the testing in real world conditions and the possible inconvenience that may be linked to their participation;

(b)the conditions under which the testing in real world conditions is to be conducted, including the expected duration of the subject or subjects' participation;

(c)their rights, and the guarantees regarding their participation, in particular their right to refuse to participate in, and the right to withdraw from, testing in real world conditions at any time without any resulting detriment and without having to provide any justification;

(d)the arrangements for requesting the reversal or the disregarding of the predictions, recommendations or decisions of the AI system;

(e)the Union-wide unique single identification number of the testing in real world conditions in accordance with Article 60(4) point (c), and the contact details of the provider or its legal representative from whom further information can be obtained.

2. The informed consent shall be dated and documented and a copy shall be given to the subjects of testing or their legal representative.

Article 62

Measures for providers and deployers, in particular SMEs, including start-ups

1. Member States shall undertake the following actions:

(a)provide SMEs, including start-ups, having a registered office or a branch in the Union, with priority access to the AI regulatory sandboxes, to the extent that they fulfil the eligibility conditions and selection criteria; the priority access shall not preclude other SMEs, including start-ups, other than those referred to in this paragraph from access to the AI regulatory sandbox, provided that they also fulfil the eligibility conditions and selection criteria;

(b)organise specific awareness raising and training activities on the application of this Regulation tailored to the needs of SMEs including start-ups, deployers and, as appropriate, local public authorities;

(c)utilise existing dedicated channels and where appropriate, establish new ones for communication with SMEs including start-ups, deployers, other innovators and, as appropriate, local public authorities to provide advice and respond to queries about the implementation of this Regulation, including as regards participation in AI regulatory sandboxes;

(d)facilitate the participation of SMEs and other relevant stakeholders in the standardisation development process.

2. The specific interests and needs of the SME providers, including start-ups, shall be taken into account when setting the fees for conformity assessment under Article 43, reducing those fees proportionately to their size, market size and other relevant indicators.

3. The AI Office shall undertake the following actions:

(a) provide standardised templates for areas covered by this Regulation, as specified by the Board in its request;

(b) develop and maintain a single information platform providing easy to use information in relation to this Regulation for all operators across the Union;

(c) organise appropriate communication campaigns to raise awareness about the obligations arising from this Regulation;

(d) evaluate and promote the convergence of best practices in public procurement procedures in relation to AI systems.

Article 63

Derogations for specific operators

1. Microenterprises 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 partner enterprises or linked enterprises within the meaning of that Recommendation. For that purpose, the Commission shall develop guidelines on the elements of the quality management system which may be complied with in a simplified manner considering the needs of microenterprises, without affecting the level of protection or the need for compliance with the requirements in respect of high-risk AI systems.

2. Paragraph 1 of this Article shall not be interpreted as exempting those operators from fulfilling any other requirements or obligations laid down in this Regulation, including those established 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 Union 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

Establishment and structure of the European Artificial Intelligence Board

1. A European Artificial Intelligence Board (the 'Board') is hereby established.

2. The Board shall be composed of one representative per Member State. The European Data Protection Supervisor shall participate as observer. The AI Office shall also attend the Board's meetings, without taking part in the votes. Other national and Union authorities, bodies or experts may be invited to the meetings by the Board on a case by case basis, where the issues discussed are of relevance for them.

3. Each representative shall be designated by their Member State for a period of three years, renewable once.

4. Member States shall ensure that their representatives on the Board:

(a) have the relevant competences and powers in their Member State so as to contribute actively to the achievement of the Board's tasks referred to in Article 66;

(b) are designated as a single contact point vis-à-vis the Board and, where appropriate, taking into account Member States' needs, as a single contact point for stakeholders;

(c) are empowered to facilitate consistency and coordination between national competent authorities in their Member State as regards the implementation of this Regulation, including through the collection of relevant data and information for the purpose of fulfilling their tasks on the Board.

5. The designated representatives of the Member States shall adopt the Board's rules of procedure by a two-thirds majority. The rules of procedure shall, in particular, lay down procedures for the selection process, the duration of the mandate of, and specifications of the tasks of, the Chair, detailed arrangements for voting, and the organisation of the Board's activities and those of its sub-groups.

6. The Board shall establish two standing sub-groups to provide a platform for cooperation and exchange among market surveillance authorities and notifying authorities about issues related to market surveillance and notified bodies respectively.

The standing sub-group for market surveillance should act as the administrative cooperation group (ADCO) for this Regulation within the meaning of Article 30 of Regulation (EU) 2019/1020.

The Board may establish other standing or temporary sub-groups as appropriate for the purpose of examining specific issues. Where appropriate, representatives of the

advisory forum referred to in Article 67 may be invited to such sub-groups or to specific meetings of those subgroups as observers.

7. The Board shall be organised and operated so as to safeguard the objectivity and impartiality of its activities.

8. The Board shall be chaired by one of the representatives of the Member States. The AI Office shall provide the secretariat for the Board, convene the meetings upon request of the Chair, and prepare the agenda in accordance with the tasks of the Board pursuant to this Regulation and its rules of procedure.

Article 66

Tasks of the Board

The Board shall advise and assist the Commission and the Member States in order to facilitate the consistent and effective application of this Regulation. To that end, the Board may in particular:

(a) contribute to the coordination among national competent authorities responsible for the application of this Regulation and, in cooperation with and subject to the agreement of the market surveillance authorities concerned, support joint activities of market surveillance authorities referred to in Article 74(11);

(b) collect and share technical and regulatory expertise and best practices among Member States;

(c) provide advice on the implementation of this Regulation, in particular as regards the enforcement of rules on general-purpose AI models;

(d) contribute to the harmonisation of administrative practices in the Member States, including in relation to the derogation from the conformity assessment procedures referred to in Article 46, the functioning of AI regulatory sandboxes, and testing in real world conditions referred to in Articles 57, 59 and 60;

(e) at the request of the Commission or on its own initiative, issue recommendations and written opinions on any relevant matters related to the implementation of this Regulation and to its consistent and effective application, including:

  (i) on the development and application of codes of conduct and codes of practice pursuant to this Regulation, as well as of the Commission's guidelines;

  (ii) the evaluation and review of this Regulation pursuant to Article 112, including as regards the serious incident reports referred to in Article 73, and the functioning of the EU database referred to in Article 71, the preparation of the delegated or implementing acts, and as regards possible alignments of this Regulation with the Union harmonisation legislation listed in Annex I;

(iii) on technical specifications or existing standards regarding 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) trends, such as European global competitiveness in AI, the uptake of AI in the Union, and the development of digital skills;

(vi) trends on the evolving typology of AI value chains, in particular on the resulting implications in terms of accountability;

(vii) on the potential need for amendment to Annex III in accordance with Article 7, and on the potential need for possible revision of Article 5 pursuant to Article 112, taking into account relevant available evidence and the latest developments in technology;

(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 a shared understanding among market operators and competent authorities of the relevant concepts provided for in this Regulation, including by contributing to the development of benchmarks;

(h) cooperate, as appropriate, with other Union institutions, bodies, offices and agencies, as well as relevant Union expert groups and networks, in particular in the fields of product safety, cybersecurity, competition, digital and media services, financial services, consumer protection, data and fundamental rights protection;

(i) contribute to effective cooperation with the competent authorities of third countries and with international organisations;

(j) assist national competent authorities and the Commission in developing the organisational and technical expertise required for the implementation of this Regulation, including by contributing to the assessment of training needs for staff of Member States involved in implementing this Regulation;

(k) assist the AI Office in supporting national competent authorities in the establishment and development of AI regulatory sandboxes, and facilitate cooperation and information-sharing among AI regulatory sandboxes;

(l) contribute to, and provide relevant advice on, the development of guidance documents;

(m) advise the Commission in relation to international matters on AI;

(n) provide opinions to the Commission on the qualified alerts regarding general-purpose AI models;

(o)receive opinions by the Member States on qualified alerts regarding general-purpose AI models, and on national experiences and practices on the monitoring and enforcement of AI systems, in particular systems integrating the general-purpose AI models.

Article 67

Advisory forum

1. An advisory forum shall be established to provide technical expertise and advise the Board and the Commission, and to contribute to their tasks under this Regulation.

2. The membership of the advisory forum shall represent a balanced selection of stakeholders, including industry, start-ups, SMEs, civil society and academia. The membership of the advisory 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 undertakings.

3. The Commission shall appoint the members of the advisory forum, in accordance with the criteria set out in paragraph 2, from amongst stakeholders with recognised expertise in the field of AI.

4. The term of office of the members of the advisory forum shall be two years, which may be extended by up to no more than four years.

5. The Fundamental Rights Agency, ENISA, the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC), and the European Telecommunications Standards Institute (ETSI) shall be permanent members of the advisory forum.

6. The advisory forum shall draw up its rules of procedure. It shall elect two co-chairs from among its members, in accordance with criteria set out in paragraph 2. The term of office of the co-chairs shall be two years, renewable once.

7. The advisory forum shall hold meetings at least twice a year. The advisory forum may invite experts and other stakeholders to its meetings.

8. The advisory forum may prepare opinions, recommendations and written contributions at the request of the Board or the Commission.

9. The advisory forum may establish standing or temporary sub-groups as appropriate for the purpose of examining specific questions related to the objectives of this Regulation.

10. The advisory forum shall prepare an annual report on its activities. That report shall be made publicly available.

Article 68

Scientific panel of independent experts

1. The Commission shall, by means of an implementing act, make provisions on the establishment of a scientific panel of independent experts (the 'scientific panel') intended to support the enforcement activities under this Regulation. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 98(2).

2. The scientific panel shall consist of experts selected by the Commission on the basis of up-to-date scientific or technical expertise in the field of AI necessary for the tasks set out in paragraph 3, and shall be able to demonstrate meeting all of the following conditions:

(a) having particular expertise and competence and scientific or technical expertise in the field of AI;

(b) independence from any provider of AI systems or general-purpose AI models;

(c) an ability to carry out activities diligently, accurately and objectively.

The Commission, in consultation with the Board, shall determine the number of experts on the panel in accordance with the required needs and shall ensure fair gender and geographical representation.

3. The scientific panel shall advise and support the AI Office, in particular with regard to the following tasks:

(a) supporting the implementation and enforcement of this Regulation as regards general-purpose AI models and systems, in particular by:

  (i) alerting the AI Office of possible systemic risks at Union level of general-purpose AI models, in accordance with Article 90;

  (ii) contributing to the development of tools and methodologies for evaluating capabilities of general-purpose AI models and systems, including through benchmarks;

  (iii) providing advice on the classification of general-purpose AI models with systemic risk;

  (iv) providing advice on the classification of various general-purpose AI models and systems;

  (v) contributing to the development of tools and templates;

(b) supporting the work of market surveillance authorities, at their request;

(c) supporting cross-border market surveillance activities as referred to in Article 74(11), without prejudice to the powers of market surveillance authorities;

(d) supporting the AI Office in carrying out its duties in the context of the Union safeguard procedure pursuant to Article 81.

4. The experts on the scientific panel shall perform their tasks with impartiality and objectivity, and shall ensure the confidentiality of information and data obtained in carrying out their tasks and activities. They shall neither seek nor take instructions from anyone when exercising their tasks under paragraph 3. Each expert shall draw up a declaration of interests, which shall be made publicly available. The AI 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 panel and its members to issue alerts, and to request the assistance of the AI Office for the performance of the tasks of the scientific panel.

Article 69

Access to the pool of experts by the Member States

1. Member States may call upon experts of the scientific panel to support their enforcement activities under this Regulation.

2. The Member States may be required to pay fees for the advice and support provided by the experts. The structure and the level of fees as well as the scale and structure of recoverable costs shall be set out in the implementing act referred to in Article 68(1), taking into account the objectives of the adequate implementation of this Regulation, cost-effectiveness and the necessity of ensuring effective access to experts for all Member States.

3. The Commission shall facilitate timely access to the experts by the Member States, as needed, and ensure that the combination of support activities carried out by Union AI testing support pursuant to Article 84 and experts pursuant to this Article is efficiently organised and provides the best possible added value.

SECTION 2

National competent authorities

Article 70

Designation of national competent authorities and single points of contact

1. Each Member State shall establish or designate as national competent authorities at least one notifying authority and at least one market surveillance authority for the purposes of this Regulation. Those national competent authorities shall exercise their powers independently, impartially and without bias so as to safeguard the objectivity of their activities and tasks, and to ensure the application and implementation of this

Regulation. The members of those authorities shall refrain from any action incompatible with their duties. Provided that those principles are observed, such activities and tasks may be performed 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, as well as any subsequent changes thereto. Member States shall make publicly available information on how competent authorities and single points of contact can be contacted, through electronic communication means by 2 August 2025. Member States shall designate a market surveillance authority to act as the single point of contact for this Regulation, and shall notify the Commission of the identity of the single point of contact. The Commission shall make a list of the single points of contact publicly available.

3. Member States shall ensure that their national competent authorities are provided with adequate technical, financial and human resources, and with infrastructure to fulfil their tasks effectively under this Regulation. In particular, the national competent authorities shall have a sufficient number of personnel permanently available whose competences and expertise shall include an in-depth understanding of AI technologies, data and data computing, personal data protection, cybersecurity, fundamental rights, health and safety risks and knowledge of existing standards and legal requirements. Member States shall assess and, if necessary, update competence and resource requirements referred to in this paragraph on an annual basis.

4. National competent authorities shall take appropriate measures to ensure an adequate level of cybersecurity.

5. When performing their tasks, the national competent authorities shall act in accordance with the confidentiality obligations set out in Article 78.

6. By 2 August 2025, and once every two years thereafter, Member States shall report to the Commission on the status of the financial and human resources of the national competent authorities, with an assessment of their adequacy. The Commission shall transmit that information to the Board for discussion and possible recommendations.

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

8. National competent authorities may provide guidance and advice on the implementation of this Regulation, in particular to SMEs including start-ups, taking into account the guidance and advice of the Board and the Commission, as appropriate. Whenever national competent authorities intend to provide guidance and advice with regard to an AI system in areas covered by other Union law, the national competent authorities under that Union law shall be consulted, as appropriate.

9. Where Union institutions, bodies, offices or 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 shall, in collaboration with the Member States, set up and maintain an EU database containing information referred to in paragraphs 2 and 3 of this Article concerning high-risk AI systems referred to in Article 6(2) which are registered in accordance with Articles 49 and 60 and AI systems that are not considered as high-risk pursuant to Article 6(3) and which are registered in accordance with Article 6(4) and Article 49. When setting the functional specifications of such database, the Commission shall consult the relevant experts, and when updating the functional specifications of such database, the Commission shall consult the Board.

2. The data listed in Sections A and B of Annex VIII shall be entered into the EU database by the provider 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 the deployer who is, or who acts on behalf of, a public authority, agency or body, 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), point (c), the information contained in the EU database registered in accordance with Article 49 shall be accessible and publicly available in a user-friendly manner. The information should be easily navigable and machine-readable. The information registered in accordance with Article 60 shall be accessible only to market surveillance authorities and the Commission, unless the prospective provider or provider has given consent for also making the information accessible the public.

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

6. The Commission shall be the controller of the EU database. It shall make available to providers, prospective providers and deployers adequate technical and administrative support. The EU database shall comply with the applicable accessibility requirements.

CHAPTER IX
POST-MARKET MONITORING, INFORMATION SHARING AND MARKET SURVEILLANCE

SECTION 1
Post-market monitoring

Article 72

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

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

2. The post-market monitoring system shall actively and systematically collect, document and analyse relevant data which may be provided by deployers or which may be collected through other sources on the performance of high-risk AI systems throughout their lifetime, and which allow the provider to evaluate the continuous compliance of AI systems with the requirements set out in Chapter III, Section 2. Where relevant, post-market monitoring shall include an analysis of the interaction with other AI systems. This obligation shall not cover sensitive operational data of deployers which are law-enforcement authorities.

3. The post-market monitoring system shall be based on a post-market monitoring plan. The post-market monitoring plan shall be part of the technical documentation referred to in Annex IV. The Commission shall adopt an implementing act laying down detailed provisions establishing a template for the post-market monitoring plan and the list of elements to be included in the plan 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 covered by the Union harmonisation legislation listed in Section A of Annex I, where a post-market monitoring system and plan are already established under that legislation, in order to ensure consistency, avoid duplications and minimise additional burdens, providers shall have a choice of integrating, as appropriate, the necessary elements described in paragraphs 1, 2 and 3 using the template referred in paragraph 3 into systems and plans already existing 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 that are subject to requirements under Union financial services law regarding their internal governance, arrangements or processes.

SECTION 2

Sharing of information on serious incidents

Article 73

Reporting of serious incidents

1. Providers of high-risk AI systems placed on the Union market shall report any serious incident to the market surveillance authorities of the Member States where that incident occurred.

2. The report 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 of such a link, and, in any event, not later than 15 days after the provider or, where applicable, the deployer, becomes aware of the serious incident.

The period for the reporting referred to in the first subparagraph shall take account of the severity of the serious incident.

3. Notwithstanding paragraph 2 of this Article, in the event of a widespread infringement or a serious incident as defined in Article 3, point (49)(b), the report referred to in paragraph 1 of this Article shall be provided immediately, and not later than two days after the provider or, where applicable, the deployer becomes aware of that incident.

4. Notwithstanding paragraph 2, in the event of the death of a person, the report shall be provided immediately after the provider or the deployer has established, or as soon as it suspects, a causal relationship between the high-risk AI system and the serious incident, but not later than 10 days after the date on which the provider or, where applicable, the deployer becomes aware of the serious incident.

5. Where necessary to ensure timely reporting, the provider or, where applicable, the deployer, may submit an initial report that is incomplete, followed by a complete report.

6. Following the reporting of a serious incident pursuant to paragraph 1, the provider shall, without delay, perform the necessary investigations in relation to the serious incident and the AI system concerned. This shall include a risk assessment of the incident, and corrective action.

The provider shall cooperate with the competent authorities, and where relevant with the notified body concerned, during the investigations referred to in the first subparagraph, and shall not perform any investigation which involves altering the AI

system concerned in a way which may affect any subsequent evaluation of the causes of the incident, prior to informing the competent authorities of such action.

7. Upon receiving a notification related to a serious incident referred to in Article 3, point (49)(c), the relevant market surveillance authority shall inform the national public authorities or bodies referred to in Article 77(1). The Commission shall develop dedicated guidance to facilitate compliance with the obligations set out in paragraph 1 of this Article. That guidance shall be issued by 2 August 2025, and shall be assessed regularly.

8. The market surveillance authority shall take appropriate measures, as provided for in Article 19 of Regulation (EU) 2019/1020, within seven days from the date it received the notification referred to in paragraph 1 of this Article, and shall follow the notification procedures as provided in that Regulation.

9. For high-risk AI systems referred to in Annex III that are placed on the market or put into service by providers that are subject to Union legislative instruments laying down reporting obligations equivalent to those set out in this Regulation, the notification of serious incidents shall be limited to those referred to in Article 3, point (49)(c).

10. For high-risk AI systems which are safety components of devices, or are themselves devices, covered by Regulations (EU) 2017/745 and (EU) 2017/746, the notification of serious incidents shall be limited to those referred to in Article 3, point (49)(c) of this Regulation, and shall be made to the national competent authority chosen for that purpose by the Member States where the incident occurred.

11. National competent authorities shall immediately notify the Commission of any serious incident, whether or not they have taken action on it, in accordance with Article 20 of Regulation (EU) 2019/1020.

SECTION 3

Enforcement

Article 74

Market surveillance and control of AI systems in the Union market

1. Regulation (EU) 2019/1020 shall apply to AI systems covered by this Regulation. For the purposes of the effective enforcement of this Regulation:

(a) any reference to an economic operator under Regulation (EU) 2019/1020 shall be understood as including all operators identified in Article 2(1) of this Regulation;

(b) any reference to a product under Regulation (EU) 2019/1020 shall be understood as including 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, the market surveillance authorities shall report annually to the Commission and relevant national competition authorities any information identified in the course of market surveillance activities that may be of potential interest for the application of Union law on competition rules. They shall also annually report to the Commission about the use of prohibited practices that occurred during that year and about the measures taken.

3. For high-risk AI systems related to products covered by the Union harmonisation legislation 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 under those legal acts.

By derogation from the first subparagraph, and in appropriate circumstances, Member States may designate another relevant authority to act as a market surveillance authority, provided they ensure coordination with the relevant sectoral market surveillance authorities responsible for the enforcement of the Union harmonisation legislation listed in Annex I.

4. The procedures referred to in Articles 79 to 83 of this Regulation shall not apply to AI systems related to products covered by the Union harmonisation legislation listed in section A of Annex I, where such legal acts already provide for procedures ensuring an equivalent level of protection and having the same objective. In such cases, the relevant sectoral procedures shall apply instead.

5. Without prejudice to the powers of market surveillance authorities under Article 14 of Regulation (EU) 2019/1020, for the purpose of ensuring the effective enforcement of this Regulation, market surveillance authorities may exercise the powers referred to in Article 14(4), points (d) and (j), of that Regulation remotely, as appropriate.

6. For high-risk AI systems placed on the market, put into service, or used by financial institutions regulated by 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 those institutions under that legislation in so far as the placing on the market, putting into service, or the use of the AI system is in direct connection with the provision of those financial services.

7. By way of derogation from paragraph 6, in appropriate circumstances, and provided that coordination is ensured, another relevant authority may be identified by the Member State as market surveillance authority for the purposes of this Regulation.

National market surveillance authorities supervising regulated credit institutions regulated under Directive 2013/36/EU, which are participating in the Single Supervisory Mechanism established by Regulation (EU) No 1024/2013, should report, without delay, to the European Central Bank any information identified in the course of

their market surveillance activities that may be of potential interest for the prudential supervisory 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, in so far as the systems are used for law enforcement purposes, 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 under Regulation (EU) 2016/679 or Directive (EU) 2016/680, or any other authority designated pursuant to the same conditions laid down 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 when acting in their judicial capacity.

9. Where Union institutions, bodies, offices or 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 acting in its judicial capacity.

10. Member States shall facilitate coordination between market surveillance authorities designated under this Regulation and other relevant national authorities or bodies which supervise the application of Union harmonisation legislation listed in Annex I, or in other Union law, that might be relevant for the high-risk AI systems referred to in Annex III.

11. Market surveillance authorities and the Commission shall be able to propose joint activities, including joint investigations, to be conducted by either market surveillance authorities or market surveillance authorities jointly with the Commission, that have the aim of promoting compliance, identifying non-compliance, raising awareness or providing guidance in relation to this Regulation with respect to specific categories of high-risk AI systems that are found to present a serious risk across two or more Member States in accordance with Article 9 of Regulation (EU) 2019/1020. The AI Office shall provide coordination support for joint investigations.

12. Without prejudice to the powers provided for under Regulation (EU) 2019/1020, and where relevant and limited to what is necessary to fulfil their tasks, the market surveillance authorities shall be granted full access by providers to the documentation as well as the 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 (API) or other relevant technical means and tools enabling remote access.

13. Market surveillance authorities shall be granted access to the source code of the high-risk AI system upon a reasoned request and only when both of the following conditions are fulfilled:

(a)access to source code is necessary to assess the conformity of a high-risk AI system with the requirements set out in Chapter III, Section 2; and

(b)testing or auditing procedures and verifications based on the data and documentation provided by the provider have been exhausted or proved 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 the model and the system are developed by the same provider, the AI Office shall have powers to monitor and supervise compliance of that AI system with obligations under this Regulation. To carry out its monitoring and supervision tasks, the AI Office shall have all the powers of a market surveillance authority provided for in this Section and Regulation (EU) 2019/1020.

2. Where the relevant market surveillance authorities have sufficient reason to consider general-purpose AI systems that can be used directly by deployers for at least one purpose that is classified as high-risk pursuant to this Regulation to be non-compliant with the requirements laid down in this Regulation, they shall cooperate with the AI Office to carry out compliance evaluations, and shall inform the Board and other market surveillance authorities accordingly.

3. Where a market surveillance authority is unable to conclude its investigation of the high-risk AI system because of its inability to access certain information related 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, by which access to that information shall be enforced. In that case, the AI Office shall supply to the applicant authority without delay, and in any event within 30 days, any information that the AI Office considers to be relevant in order to establish whether a high-risk AI system is non-compliant. Market surveillance authorities shall safeguard the confidentiality of the information that they obtain in accordance with Article 78 of this Regulation. The procedure provided for in Chapter VI of Regulation (EU) 2019/1020 shall apply *mutatis mutandis*.

Article 76

Supervision of testing in real world conditions by market surveillance authorities

1. Market surveillance authorities shall have competences and powers to ensure that testing in real world conditions is in accordance with this Regulation.

2. Where testing in real world conditions is conducted for AI systems that are supervised within an AI regulatory sandbox under Article 58, the market surveillance authorities shall verify the compliance with Article 60 as part of their supervisory role for the AI regulatory sandbox. Those authorities may, as appropriate, allow the testing in real world conditions to be conducted by the provider or prospective provider, in derogation from the conditions set out in Article 60(4), points (f) and (g).

3. Where a market surveillance authority has been informed by the prospective provider, the provider or any third party of a serious incident or has other grounds for considering that the conditions set out in Articles 60 and 61 are not met, it may take either of the following decisions on its territory, as appropriate:

(a) to suspend or terminate the testing in real world conditions;

(b) to require the provider or prospective provider and the deployer or prospective deployer to modify any aspect of the testing in real world conditions.

4. Where a market surveillance authority has taken a decision referred to in paragraph 3 of this Article, or has issued an objection within the meaning of Article 60(4), point (b), the decision or the objection shall indicate the grounds therefor and how the provider or prospective provider can challenge the decision or objection.

5. Where applicable, where a market surveillance authority has taken a decision referred to in paragraph 3, it shall communicate the grounds therefor to the market surveillance authorities of other Member States in which the AI system has been tested in accordance with the testing plan.

Article 77

Powers of authorities protecting fundamental rights

1. National public authorities or bodies which supervise or enforce the respect of obligations under Union law protecting fundamental rights, including the right to non-discrimination, in relation to the use of high-risk AI systems referred to in Annex III shall have the power to request and access any documentation created or maintained under this Regulation in accessible language and format when access to that documentation is necessary for effectively fulfilling their mandates within the limits of their jurisdiction. The relevant public authority or body shall inform the market surveillance authority of the Member State concerned of any such request.

2. By 2 November 2024, each Member State shall identify the public authorities or bodies referred to in paragraph 1 and make a list of them publicly available. Member

States shall notify the list to the Commission and to the other Member States, and shall keep the list up to date.

3. Where the documentation referred to in paragraph 1 is insufficient to ascertain whether an infringement of obligations under Union law protecting fundamental rights has occurred, the public authority or body referred to in paragraph 1 may make a reasoned request to the market surveillance authority, to organise testing of the high-risk AI system through technical means. The market surveillance authority shall organise the testing with the close involvement of the requesting public authority or body within a reasonable time following the request.

4. Any information or documentation obtained by the 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 set out in Article 78.

Article 78

Confidentiality

1. The Commission, market surveillance authorities and notified bodies and any other natural or legal person involved in the application of this Regulation shall, in accordance with Union or national law, respect the confidentiality of information and data obtained in carrying out their tasks and activities in such a manner as to protect, in particular:

(a) the intellectual 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 implementation of this Regulation, in particular for the purposes of inspections, investigations or audits;

(c) public and national security interests;

(d) the conduct of criminal or administrative proceedings;

(e) information classified pursuant to Union or national law.

2. The authorities involved in the application of this Regulation pursuant to paragraph 1 shall request only data that is strictly necessary for the assessment of the risk posed by AI systems and for the exercise of their powers in accordance with this Regulation and with Regulation (EU) 2019/1020. They shall put in place adequate and effective cybersecurity measures to protect the security and confidentiality of the information and data obtained, and shall delete the data collected as soon as it is no longer needed for the purpose for which it was obtained, in accordance with applicable Union or national law.

3. Without prejudice to paragraphs 1 and 2, information exchanged on a confidential basis between the national competent authorities or between national competent authorities and the Commission shall not be disclosed without prior consultation of the originating national competent authority and the deployer when high-risk AI systems referred to in point 1, 6 or 7 of Annex III are used by law enforcement, border control, immigration or asylum authorities and when such disclosure would jeopardise public and national security interests. This exchange of information shall not cover sensitive operational data in relation to the activities of law enforcement, border control, immigration or asylum authorities.

When the law enforcement, immigration or asylum authorities are providers of high-risk AI systems referred to in point 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 applicable, can, upon request, immediately access the documentation or obtain a copy thereof. Only staff of the market surveillance authority holding the appropriate level of security clearance shall be allowed to access that documentation or any copy thereof.

4. Paragraphs 1, 2 and 3 shall not affect the rights or obligations of the Commission, Member States and their relevant authorities, as well as those of notified bodies, with regard to the exchange of information and the dissemination of warnings, including in the context of cross-border cooperation, nor shall they affect the obligations of the parties concerned to provide information under criminal law of the Member States.

5. The Commission and Member States may exchange, where necessary and in accordance with relevant provisions of international and trade agreements, confidential information with regulatory authorities of third countries with which they have concluded bilateral or multilateral confidentiality arrangements guaranteeing an adequate level of confidentiality.

Article 79

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

1. AI systems presenting a risk shall be understood as a ‘product presenting a risk’ as defined in Article 3, point 19 of Regulation (EU) 2019/1020, in so far as they present risks to the health or safety, or to fundamental rights, of persons.

2. Where the market surveillance authority of a Member State has sufficient reason to consider an AI system to present a risk as referred to in paragraph 1 of this Article, it shall carry out an evaluation of the AI system concerned in respect of its compliance with all the requirements and obligations laid down in this Regulation. Particular attention shall be given to AI systems presenting a risk to vulnerable groups. Where risks to fundamental rights are identified, the market surveillance authority shall also

inform and fully cooperate with the relevant national public authorities or bodies referred to in Article 77(1). The 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).

Where, in the course of that evaluation, 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 laid down in this Regulation, it shall without undue delay require the relevant operator to take all appropriate corrective actions to bring the AI system into compliance, to withdraw the AI system from the market, or to recall it within a period the market surveillance authority may prescribe, and in any event within the shorter of 15 working days, or as provided for in the relevant Union harmonisation legislation.

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 restricted to its national territory, it shall inform the Commission and the other Member States without undue delay of the results of the evaluation and of the actions which it has required the operator to take.

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

5. Where the operator of an AI system does not take adequate corrective action within the period referred to in paragraph 2, the market surveillance authority shall take all appropriate provisional measures to prohibit or restrict the AI system's being made available on its national market or put into service, to withdraw the product or the standalone AI system from that market or to recall it. That authority shall without undue delay notify the Commission and the other Member States of those measures.

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 non-compliance alleged and the risk involved, the nature and duration of the national measures taken and the arguments put forward by the relevant operator. In particular, the market surveillance authorities shall indicate whether the non-compliance is due to one or more of the following:

(a) non-compliance with the prohibition of the AI practices referred to in Article 5;

(b) a failure of a high-risk AI system to meet requirements set out in Chapter III, Section 2;

(c) shortcomings in the harmonised standards or common specifications referred to in Articles 40 and 41 conferring a presumption of conformity;

(d) non-compliance with Article 50.

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

8. Where, within three months of receipt of the notification referred to in paragraph 5 of this Article, no objection has been raised by either a market surveillance authority of a Member State or by the Commission in respect of a provisional measure taken by a market surveillance authority of another Member State, that measure shall be deemed justified. This shall be without prejudice to the procedural rights of the concerned operator in accordance with Article 18 of Regulation (EU) 2019/1020. The three-month period referred to in this paragraph shall be reduced to 30 days in the event of non-compliance with the prohibition of the AI practices referred to in Article 5 of this Regulation.

9. The market surveillance authorities shall ensure that appropriate restrictive measures are taken in respect of the product or the AI system concerned, such as withdrawal of the product or the AI system from their market, without undue delay.

Article 80

Procedure for dealing with AI systems classified by the provider as non-high-risk in application of Annex III

1. Where a market surveillance authority has sufficient reason to consider that an AI system classified by the provider as non-high-risk pursuant to Article 6(3) is indeed high-risk, the market surveillance authority shall carry out an evaluation of the AI system concerned in respect of its classification as a high-risk AI system based on the conditions set out in Article 6(3) and the Commission guidelines.

2. Where, in the course of that evaluation, 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 necessary actions to bring the AI system into compliance with the requirements and obligations laid down in this Regulation, as well as take appropriate corrective action within a period the market surveillance authority may prescribe.

3. Where the market surveillance authority considers that the use of the AI system concerned is not restricted to its national territory, it shall inform the Commission and

the other Member States without undue delay of the results of the evaluation and of the actions which it has required the provider to take.

4. The provider shall ensure that all necessary action is taken to bring the AI system into compliance with the requirements and obligations laid down in this Regulation. Where the provider of an AI system concerned does not bring the AI system into compliance with those requirements and obligations within the period referred to in paragraph 2 of this Article, the provider shall be subject to fines in accordance with Article 99.

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

6. Where the provider of the AI system concerned does not take adequate corrective action within the period referred to in paragraph 2 of this Article, Article 79(5) to (9) shall apply.

7. Where, in the course of the evaluation pursuant to paragraph 1 of this Article, the market surveillance authority establishes that the AI system was misclassified by the provider as non-high-risk in order to circumvent the application of requirements in Chapter III, Section 2, the provider shall be subject to fines in accordance with Article 99.

8. In exercising their power to monitor the application of this Article, and in accordance with Article 11 of Regulation (EU) 2019/1020, market surveillance authorities may perform appropriate checks, taking into account in particular 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 case of non-compliance with the prohibition of the AI practices referred to in Article 5, objections are raised by the market surveillance authority of a Member State to a measure taken by another market surveillance authority, or where the Commission considers the measure to be contrary to Union law, the Commission shall without undue delay enter into consultation with the market surveillance authority of the relevant Member State and the operator or operators, and shall evaluate the national measure. On the basis of the results of that evaluation, the Commission shall, within six months, or within 60 days in the case of non-compliance with the prohibition of the AI practices referred to in Article 5, starting from the notification referred to in Article 79(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 shall also inform all other market surveillance authorities of its decision.

2. Where the Commission considers the measure taken by the relevant Member State to be justified, all Member States shall ensure that they take appropriate restrictive measures in respect of the AI system concerned, such as requiring the withdrawal of the AI system from their market without undue delay, and shall inform the Commission accordingly. Where the Commission considers the national measure to be unjustified, the Member State concerned shall withdraw the measure and shall inform the Commission accordingly.

3. Where the national measure is considered justified and the non-compliance of the AI system is attributed to shortcomings 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 1025/2012.

Article 82

Compliant AI systems which present a risk

1. Where, having performed an evaluation under Article 79, after consulting the relevant national public authority referred to in Article 77(1), the market surveillance authority of a Member State finds that although a high-risk AI system complies with this Regulation, it nevertheless presents a risk to the health or safety of persons, to fundamental rights, or to other aspects of public interest protection, it shall require the relevant operator to take all appropriate measures to ensure that the AI system concerned, when placed on the market or put into service, no longer presents that risk without undue delay, within a period it may prescribe.

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

3. The Member States shall immediately inform the Commission and the other Member States of a finding under paragraph 1. That information shall include all available details, in particular the data necessary for the identification of the AI system concerned, the origin and the supply chain of the AI system, the nature of the risk involved and the nature and duration of the national measures taken.

4. The Commission shall without undue delay enter into consultation with the Member States concerned and the relevant operators, and shall evaluate the national measures taken. On the basis of the results of that evaluation, the Commission shall decide whether the measure is justified and, where necessary, 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 makes one of the following findings, it shall require the relevant provider to put an end to the non-compliance concerned, within a period it may prescribe:

(a) the CE marking has been affixed in violation of Article 48;

(b) the CE marking has not been affixed;

(c) the EU declaration of conformity referred to in Article 47 has not been drawn up;

(d) the EU declaration of conformity referred to in Article 47 has not been drawn up correctly;

(e) the registration in the EU database referred to in Article 71 has not been carried out;

(f) where applicable, no authorised representative has been appointed;

(g) technical documentation is not available.

2. Where 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 high-risk AI system being made available on the market or to ensure that it is recalled or withdrawn from the market without delay.

Article 84

Union AI testing support structures

1. The Commission shall designate one or more Union AI testing support structures to perform the tasks listed under Article 21(6) of Regulation (EU) 2019/1020 in the area of AI.

2. Without prejudice to the tasks referred to in paragraph 1, Union AI testing support structures shall also provide independent technical or scientific advice at the request of the Board, the Commission, or of market surveillance authorities.

SECTION 4

Remedies

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 having grounds to consider that there has been an infringement of the provisions of this Regulation may submit complaints to the relevant market surveillance authority.

In accordance with Regulation (EU) 2019/1020, such complaints shall be taken into account for the purpose of conducting market surveillance activities, and shall be handled in line with the dedicated procedures established therefor by the market surveillance authorities.

Article 86

Right to explanation of individual decision-making

1. Any affected person subject to a decision which is taken by the deployer on the basis of the output from a high-risk AI system listed in Annex III, with the exception of systems listed under point 2 thereof, and which produces legal effects or similarly significantly affects that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights shall have the right to obtain from the deployer clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken.

2. Paragraph 1 shall not apply to the use of AI systems for which exceptions from, or restrictions to, the obligation under that paragraph follow from Union or national law in compliance 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 under Union law.

Article 87

Reporting of infringements and protection of reporting persons

Directive (EU) 2019/1937 shall apply to the reporting of infringements of this Regulation and the protection of persons reporting such infringements.

SECTION 5

Supervision, investigation, enforcement and monitoring in respect of providers of general-purpose AI models

Article 88

Enforcement of the obligations of providers of general-purpose AI models

1. The Commission shall have exclusive powers to supervise and enforce Chapter V, taking into account the procedural guarantees under Article 94. The Commission shall

entrust the implementation of these tasks to the AI Office, without prejudice to the powers of organisation of the Commission and the division of competences between Member States and the Union based on the Treaties.

2. Without prejudice to Article 75(3), market surveillance authorities may request the Commission to exercise the powers laid down in this Section, where that is necessary and proportionate to assist with the fulfilment of their tasks under this Regulation.

Article 89

Monitoring actions

1. For the purpose of carrying out the tasks assigned to it under this Section, the AI Office may take the necessary actions to monitor the effective implementation and compliance with this Regulation by providers of general-purpose AI models, including their adherence to approved codes of practice.

2. Downstream providers shall have the right to lodge a complaint alleging an infringement of this Regulation. A complaint shall be duly reasoned and indicate at least:

(a) the point of contact of the provider of the general-purpose AI model concerned;

(b) a description of the relevant facts, the provisions of this Regulation concerned, and the reason why the downstream provider considers that the provider of the general-purpose AI model concerned infringed this Regulation;

(c) any other information that the downstream provider that sent the request considers relevant, including, where appropriate, information gathered on its own initiative.

Article 90

Alerts of systemic risks by the scientific panel

1. The scientific panel may provide a qualified alert to the AI Office where it has reason to suspect that:

(a) a general-purpose AI model poses concrete identifiable risk at Union level; or

(b) a general-purpose AI model meets the conditions referred to in Article 51.

2. Upon such qualified alert, the Commission, through the AI Office and after having informed the Board, may exercise the powers laid down in this Section for the purpose of assessing the matter. The AI Office shall inform the Board of any measure according to Articles 91 to 94.

3. A qualified alert shall be duly reasoned and indicate at least:

(a) the point of contact of the provider of the general-purpose AI model with systemic risk concerned;

(b) a description of the relevant facts and the reasons for the alert by the scientific panel;

(c) any other information that the scientific panel considers to be relevant, including, where appropriate, information gathered on its own initiative.

Article 91

Power to request documentation and information

1. The Commission may request the provider of the general-purpose AI model concerned to provide the documentation drawn up by the provider in accordance with Articles 53 and 55, or any additional information that is necessary for the purpose of assessing compliance of the provider with this Regulation.

2. Before sending the request for information, the AI Office may initiate a structured dialogue with the provider of the general-purpose AI model.

3. Upon a duly substantiated request from the scientific panel, the Commission may issue a request for information to a provider of a general-purpose AI model, where the access to information is necessary and proportionate for the fulfilment of the tasks of the scientific panel under Article 68(2).

4. The request for information shall state the legal basis and the purpose of the request, specify what information is required, set a period within which the information is to be provided, and indicate the fines provided for in Article 101 for supplying incorrect, incomplete or misleading information.

5. The provider of the general-purpose AI model concerned, or its representative shall supply the information requested. In the case of legal persons, companies or firms, or where the provider has no legal personality, the persons authorised to represent them by law or by their statutes, shall supply the information requested on behalf of the provider of the general-purpose AI model concerned. Lawyers duly authorised to act may supply information on behalf of their clients. The clients shall nevertheless remain fully responsible if the information supplied is incomplete, incorrect or misleading.

Article 92

Power to conduct evaluations

1. The AI Office, after consulting the Board, may conduct evaluations of the general-purpose AI model concerned:

(a) to assess compliance of the provider with obligations under this Regulation, where the information gathered pursuant to Article 91 is insufficient; or

(b) to investigate systemic risks at Union level of general-purpose AI models with systemic risk, in particular following a qualified alert from the scientific panel in accordance with Article 90(1), point (a).

2. The Commission may decide to appoint independent experts to carry out evaluations on its behalf, including from the scientific panel established pursuant to Article 68. Independent experts appointed for this task shall meet the criteria outlined in Article 68(2).

3. For the purposes of paragraph 1, the Commission may request access to the general-purpose AI model concerned through APIs or further appropriate technical means and tools, including source code.

4. The request for access shall state the legal basis, the purpose and reasons of the request and set the period within which the access is to be provided, and the fines provided for in Article 101 for failure to provide access.

5. The providers of the general-purpose AI model concerned or its representative shall supply the information requested. In the case of legal persons, companies or firms, or where the provider has no legal personality, the persons authorised to represent them by law or by their statutes, shall provide the access requested on behalf of the provider of the general-purpose AI model concerned.

6. The Commission shall adopt implementing acts setting out the detailed arrangements and the conditions for the evaluations, including the detailed arrangements for involving independent experts, and the procedure for the selection thereof. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

7. Prior to requesting access to the general-purpose AI model concerned, the AI Office may initiate a structured dialogue with the provider of the general-purpose AI model to gather more information on the internal testing of the model, internal safeguards for preventing systemic risks, and other internal procedures and measures the provider has taken to mitigate such risks.

Article 93

Power to request measures

1. Where necessary and appropriate, the Commission may request providers to:

(a) take appropriate measures to comply with the obligations set out in Articles 53 and 54;

(b) implement mitigation measures, where the evaluation carried out in accordance with Article 92 has given rise to serious and substantiated concern of a systemic risk at Union level;

(c) restrict the making available on the market, withdraw or recall the model.

2. Before a measure is requested, the AI Office may initiate 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 offers commitments to implement mitigation measures to address a systemic risk at Union level, the Commission may, by decision, make those commitments binding and declare that there are no further grounds for action.

Article 94

Procedural rights of economic operators of the general-purpose AI model

Article 18 of Regulation (EU) 2019/1020 shall apply *mutatis mutandis* to the providers of the general-purpose AI model, without prejudice to more specific procedural rights provided for in this Regulation.

CHAPTER X
CODES OF CONDUCT AND GUIDELINES

Article 95

Codes of conduct for voluntary application of specific requirements

1. The AI Office and the Member States shall encourage and facilitate the drawing up of codes of conduct, including related governance mechanisms, intended to foster the voluntary application to AI systems, other than high-risk AI systems, of some or all of the requirements set out in Chapter III, Section 2 taking into account the available technical solutions and industry best practices allowing for the application of such requirements.

2. The AI Office and the Member States shall facilitate the drawing up of codes of conduct concerning the voluntary application, including by deployers, of specific requirements to all AI systems, on the basis of clear objectives and key performance indicators to measure the achievement of those objectives, including elements such as, but not limited to:

(a) applicable elements provided for in Union ethical guidelines for trustworthy AI;

(b) assessing and minimising the impact of AI systems on environmental sustainability, including as regards energy-efficient programming and techniques for the efficient design, training and use of AI;

(c) promoting AI literacy, in particular that of persons dealing with the development, operation and use of AI;

(d) facilitating an inclusive and diverse design of AI systems, including through the establishment of inclusive and diverse development teams and the promotion of stakeholders' participation in that process;

(e) assessing and preventing the negative impact of AI systems on vulnerable persons or groups of vulnerable persons, including as regards accessibility for persons with a disability, as well as on gender equality.

3. Codes of conduct may be drawn up by individual providers or deployers of AI systems or by organisations representing them or by both, including with the involvement of any interested stakeholders and their representative organisations, including civil society organisations and academia. Codes of conduct may cover one or more AI systems taking into account the similarity of the intended purpose of the relevant systems.

4. The AI Office and the Member States shall take into account the specific interests and needs of SMEs, including start-ups, when encouraging and facilitating the drawing up of codes of conduct.

Article 96

Guidelines from the Commission on the implementation of this Regulation

1. The Commission shall develop guidelines on the practical implementation of this Regulation, and in particular on:

(a) the application of the requirements and obligations referred to in Articles 8 to 15 and in Article 25;

(b) the prohibited practices referred to in Article 5;

(c) the practical implementation of the provisions related to substantial modification;

(d) the practical implementation of transparency obligations laid down in Article 50;

(e) detailed information on the relationship of this Regulation with the Union harmonisation legislation listed in Annex I, as well as with other relevant Union law, including as regards consistency in their enforcement;

(f) the application of the definition of an AI system as set out in Article 3, point (1).

When issuing such guidelines, the Commission shall pay particular attention to the needs of SMEs including start-ups, of local public authorities and of the 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 acknowledged state of the art on AI, as well as of relevant harmonised standards and common specifications that are referred to in Articles 40 and

41, or of those harmonised standards or technical specifications that are set out pursuant to Union harmonisation law.

2. At the request of the Member States or the AI Office, or on its own initiative, the Commission shall update guidelines previously adopted when deemed necessary.

CHAPTER XI
DELEGATION OF POWER AND COMMITTEE PROCEDURE

Article 97

Exercise of the 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) 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) 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 of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the *Official Journal of the European Union* or 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. Any 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 by either 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 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

CHAPTER XII
PENALTIES

Article 99

Penalties

1. In accordance with the terms and conditions laid down in this Regulation, Member States shall lay down the rules on penalties and other enforcement measures, which may also include warnings and non-monetary measures, applicable to infringements of this Regulation by operators, and shall take all measures necessary to ensure that they are properly and effectively implemented, thereby taking into account the guidelines issued by the Commission pursuant to Article 96. The penalties provided for shall be effective, proportionate and dissuasive. They shall take into account the interests of SMEs, including start-ups, and their economic viability.

2. The Member States shall, without delay and at the latest by the date of entry into application, notify the Commission of the rules on penalties and of other enforcement measures referred to in paragraph 1, and shall notify it, without delay, of any subsequent amendment to them.

3. Non-compliance with the prohibition of the 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 annual turnover for the preceding financial year, whichever is higher.

4. Non-compliance with any of the following provisions related to operators or notified bodies, other than those laid down in Articles 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 annual turnover for the preceding financial year, whichever is higher:

(a) obligations of providers pursuant to Article 16;

(b) obligations of authorised representatives pursuant to Article 22;

(c) obligations of importers pursuant to Article 23;

(d) obligations of distributors pursuant to Article 24;

(e) obligations of deployers pursuant to Article 26;

(f) requirements and obligations of notified bodies pursuant to Article 31, Article 33(1), (3) and (4) or Article 34;

(g) transparency obligations for providers and deployers pursuant to Article 50.

5. The supply of incorrect, incomplete or misleading information to notified bodies or national competent authorities in reply 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 its total worldwide annual turnover for the preceding financial year, whichever is higher.

6. In the case of SMEs, including start-ups, each fine referred to in this Article shall be up to the percentages or amount referred to in paragraphs 3, 4 and 5, whichever thereof is lower.

7. When deciding whether to impose an administrative fine and when deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and, as appropriate, regard shall be given to the following:

(a) the nature, gravity and duration of the infringement and of its consequences, taking into account the purpose of the AI system, as well as, where appropriate, the number of affected persons and the level of damage suffered by them;

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

(c) whether administrative fines have already been applied by other authorities to the same operator for infringements of other Union or national law, when such infringements result from the same activity or omission constituting a relevant infringement of this Regulation;

(d) the size, the 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 gained, or losses avoided, directly or indirectly, from the infringement;

(f) the degree of cooperation with the national competent authorities, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the degree of responsibility of the operator taking into account the technical and organisational measures implemented by it;

(h) the manner in which the infringement became known to the national competent authorities, in particular whether, and if so to what extent, the operator notified the infringement;

(i) the intentional or negligent character of the infringement;

(j) any action taken by the operator to mitigate the harm suffered by the affected persons.

8. Each Member State shall lay down rules on to what extent 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 manner that the fines are imposed by competent national courts or by other bodies, as applicable in those Member States. The application of such rules in those Member States shall have an equivalent effect.

10. The exercise of powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and national law, including effective judicial remedies and due process.

11. Member States shall, on an annual basis, report to the Commission about the administrative fines they have issued during that year, in accordance with this Article, and about any related litigation or judicial proceedings.

Article 100

Administrative fines on Union institutions, bodies, offices and agencies

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

(a) the nature, gravity and duration of the infringement and of its consequences, taking into account the purpose of the AI system concerned, as well as, where appropriate, the number of affected persons and the level of damage suffered by them;

(b) the degree of responsibility of the Union institution, body, office or agency, taking into account technical and organisational measures implemented by them;

(c) any action taken by the Union institution, body, office or agency to mitigate the damage suffered by affected persons;

(d) the degree of cooperation with the European Data Protection Supervisor in order to remedy the infringement and mitigate the possible adverse effects of the infringement, including compliance with any of the measures previously ordered by the European Data Protection

Supervisor against the Union institution, body, office or agency concerned with regard to the same subject matter;

(e) any similar previous infringements by the Union institution, body, office or agency;

(f) the manner in which the infringement became known to the European Data Protection Supervisor, in particular whether, and if so to what extent, the Union institution, body, office or agency notified the infringement;

(g) the annual budget of the Union institution, body, office or agency.

2. Non-compliance with the prohibition of the AI practices referred to in Article 5 shall be subject to administrative fines of up to EUR 1 500 000.

3. The non-compliance of the AI system with any requirements or obligations under this Regulation, other than those laid down in Article 5, shall be subject to administrative fines of up to EUR 750 000.

4. Before taking decisions pursuant to this Article, the European Data Protection Supervisor shall give the Union institution, body, office or agency which is the subject of the proceedings conducted by the European Data Protection Supervisor the opportunity of being heard on the matter regarding the possible infringement. The European Data Protection Supervisor shall base his or her decisions only on elements and circumstances on which the parties concerned have been able to comment. Complainants, if any, shall be associated closely with the proceedings.

5. The rights of defence of the parties concerned shall be fully respected in the proceedings. They shall be entitled to have access to the European Data Protection Supervisor's file, subject to the legitimate interest of individuals or undertakings in the protection of their personal data or business secrets.

6. Funds collected by imposition of fines in this Article shall contribute to the general budget of the Union. The fines shall not affect the effective operation of the Union institution, body, office or agency fined.

7. The European Data Protection Supervisor shall, on an annual basis, notify the Commission of the administrative fines it has imposed pursuant to this Article and of any litigation or judicial proceedings it has initiated.

Article 101

Fines for providers of general-purpose AI models

1. The Commission may impose on providers of general-purpose AI models fines not exceeding 3 % of their annual total worldwide turnover in the preceding financial year or EUR 15 000 000, whichever is higher., when the Commission finds that the provider intentionally or negligently:

(a) infringed the relevant provisions of this Regulation;

(b) failed to comply with a request for a document or for information pursuant to Article 91, or supplied incorrect, incomplete or misleading information;

(c) failed to comply with a measure requested under Article 93;

(d) failed to make available to the Commission access to the general-purpose AI model or general-purpose AI model with systemic risk with a view to conducting an evaluation pursuant to Article 92.

In fixing the amount of the fine or periodic penalty payment, regard shall be had to the nature, gravity and duration of the infringement, taking due account of the principles of proportionality and appropriateness. The Commission shall also into account commitments made in accordance with Article 93(3) or made in relevant codes of practice in accordance with Article 56.

2. Before adopting the decision pursuant to paragraph 1, the Commission shall communicate its preliminary findings to the provider of the general-purpose AI model and give it an opportunity to be heard.

3. Fines imposed in accordance with this Article shall be effective, proportionate and dissuasive.

4. Information on fines imposed under this Article shall also be communicated to the Board as appropriate.

5. The Court of Justice of the European Union shall have unlimited jurisdiction to review decisions of the Commission fixing a fine under this Article. It may cancel, reduce or increase the fine imposed.

6. The Commission shall adopt implementing acts containing detailed arrangements and procedural safeguards for proceedings in view of 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 300/2008

In Article 4(3) of Regulation (EC) No 300/2008, the following subparagraph is added:

‘When adopting detailed measures related to technical specifications and procedures for approval and use of security equipment concerning 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.

Article 103

Amendment to Regulation (EU) No 167/2013

In Article 17(5) of Regulation (EU) No 167/2013, the following subparagraph is added:

‘When adopting delegated acts pursuant to the first subparagraph concerning artificial intelligence systems which 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.

Article 104

Amendment to Regulation (EU) No 168/2013

In Article 22(5) of Regulation (EU) No 168/2013, the following subparagraph is added:

‘When adopting delegated acts pursuant to the first subparagraph concerning Artificial Intelligence systems which 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.

Article 105

Amendment to Directive 2014/90/EU

In Article 8 of Directive 2014/90/EU, the following paragraph is added:

‘5. For Artificial Intelligence systems which are safety components within the meaning of Regulation (EU) 2024/1689 of the European Parliament and of the Council (*), when carrying out its activities pursuant to paragraph 1 and when adopting technical specifications and testing standards in accordance with paragraphs 2 and 3, the Commission shall take into account the requirements set out in Chapter III, Section 2, of that Regulation.

Article 106

Amendment to Directive (EU) 2016/797

In Article 5 of Directive (EU) 2016/797, the following paragraph is added:

‘12. When adopting delegated acts pursuant to paragraph 1 and implementing acts pursuant to paragraph 11 concerning Artificial Intelligence systems which 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.

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 concerning Artificial Intelligence systems which 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.

Article 108

Amendments 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 concerning Artificial Intelligence systems which 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 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (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. When adopting delegated acts pursuant to paragraphs 1 and 2 concerning Artificial Intelligence systems which 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 concerning Artificial Intelligence systems which 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. When adopting delegated acts pursuant to paragraphs 1 and 2 concerning Artificial Intelligence systems which 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 subparagraph is added:

‘When adopting those implementing acts concerning Artificial Intelligence systems which 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.’

;

(6)in Article 58, the following paragraph is added:

‘3. When adopting delegated acts pursuant to paragraphs 1 and 2 concerning Artificial Intelligence systems which 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 the implementing acts pursuant to paragraph 2, concerning artificial intelligence systems which 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.

Article 110

Amendment to Directive (EU) 2020/1828

In Annex I to 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 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).’.

Article 111

AI systems already placed on the market or put into service and general-purpose AI models already placed on the marked

1. Without prejudice to the application of Article 5 as referred to in Article 113(3), point (a), AI systems which are components of the large-scale IT systems established by the legal acts listed in Annex X that have been placed on the market or put into service before 2 August 2027 shall be brought into compliance with this Regulation by 31 December 2030.

The requirements laid down in this Regulation shall be taken into account in the evaluation of each large-scale IT system established by the legal acts listed in Annex X to be undertaken as provided for in those legal acts and where those legal acts are replaced or amended.

2. Without prejudice to the application of Article 5 as referred to in Article 113(3), point (a), this Regulation shall apply to operators of high-risk AI systems, other than the systems 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, as from that date, those systems are subject to significant changes in their designs. In any case, the providers and deployers of high-risk AI systems intended to be used by public authorities shall take the necessary steps 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 steps in order to comply with the obligations laid down in this Regulation by 2 August 2027.

Article 112

Evaluation and review

1. The Commission shall assess the need for amendment of the list set out in Annex III and of the list of prohibited AI practices laid down in Article 5, once a year following the entry into force of this Regulation, and until the end of the period of the delegation of power laid down in Article 97. The Commission shall submit the findings of that assessment to the European Parliament and the Council.

2. By 2 August 2028 and every four years thereafter, the Commission shall evaluate and report to the European Parliament and to the Council on the following:

(a) the need for amendments extending existing area headings or adding new area headings in Annex III;

(b) amendments to the list of AI systems requiring additional transparency measures in Article 50;

(c) amendments enhancing the effectiveness of the supervision and governance system.

3. By 2 August 2029 and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The report shall include an assessment with regard to the structure of enforcement and the possible need for a Union agency to resolve any identified shortcomings. On the basis of the findings, that report shall, where appropriate, be accompanied by a proposal for amendment of this Regulation. The reports shall be made public.

4. The reports referred to in paragraph 2 shall pay specific attention to the following:

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

(b) the state of penalties, in particular administrative fines as referred to in Article 99(1), applied by Member States for infringements of this Regulation;

(c) adopted harmonised standards and common specifications developed to support this Regulation;

(d) the number of undertakings that enter the market after the entry into application of this Regulation, and how many of them are SMEs.

5. By 2 August 2028, the Commission shall evaluate the functioning of the AI Office, whether the AI Office has been given sufficient powers and competences to fulfil its tasks, and whether it would be relevant and needed for the proper implementation and enforcement of this Regulation to upgrade the AI Office and its enforcement competences and to increase its resources. The Commission shall submit a report on its evaluation to the European Parliament and to the Council.

6. By 2 August 2028 and every four years thereafter, the Commission shall submit a report on the review of the progress on the development of standardisation deliverables on the energy-efficient development of general-purpose AI models, and asses the need for further measures or actions, including binding measures or actions. The report shall be submitted to the European Parliament and to the Council, and it shall be made public.

7. By 2 August 2028 and every three years thereafter, the Commission shall evaluate the impact and effectiveness of voluntary codes of conduct to foster the application of the requirements set out in Chapter III, Section 2 for AI systems other than high-risk AI systems and possibly other additional requirements for AI systems other than high-risk AI systems, including as regards environmental sustainability.

8. For the purposes of paragraphs 1 to 7, the Board, the Member States and national competent authorities shall provide the Commission with information upon its request and without undue delay.

9. In carrying out the evaluations and reviews referred to in paragraphs 1 to 7, the Commission shall take into account the positions and findings of the Board, of the European Parliament, of the Council, and of other relevant bodies or sources.

10. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account developments in technology, the effect of AI systems on health and safety, and on fundamental rights, and in light of the state of progress in the information society.

11. To guide the evaluations and reviews referred to in paragraphs 1 to 7 of this Article, the AI Office shall undertake to develop an objective and participative methodology for the evaluation of risk levels based on the criteria outlined in the relevant Articles and the inclusion of new systems in:

(a) the list set out in Annex III, including the extension of existing area headings or the addition of new area headings 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. Any amendment to this Regulation pursuant to paragraph 10, or relevant delegated or implementing acts, which concerns sectoral Union harmonisation legislation listed in Section B of Annex I shall take into account the regulatory specificities of each sector, and the existing governance, conformity assessment and enforcement mechanisms and authorities established therein.

13. By 2 August 2031, the Commission shall carry out an assessment of the enforcement of this Regulation and shall report on it 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 the findings, that report shall, where appropriate, be accompanied by a proposal for amendment of this Regulation with regard to the structure of enforcement and the need for a Union agency to resolve any identified shortcomings.

Article 113

Entry into force and application

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

It shall apply from 2 August 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 in 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.

For the European Parliament

The President

R. METSOLA

For the Council

The President

M. MICHEL