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

Article 114 of the Treaty on the Functioning of the European Union (TFEU)
Article 16 TFEU
Recourse to Article 16 TFEU
European Data Protection Board..."

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 Article 2 of the Treaty on European Union (TEU) Article 6 TEU, the Charter

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

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

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

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

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

Article 2, point (4) of Directive (EU) 2022/2557 of the European Parliament

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

Article 16 TFEU
Article 10 of Directive (EU) 2016/680
Article 10 of Directive (EU) 2016/680
Article 8 of Directive (EU) 2016/680

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

Article 10 of Directive (EU) 2016/680
Article 9(1) of Regulation (EU) 2016/679
Article 10(1) of Regulation (EU) 2018/1725
Article 9(1) of Regulation (EU) 2016/679

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

Article 6a of Protocol No 21 on the position of the United Kingdom and Ireland
Article 5(1), first subparagraph, point (g),
Article 5(1), first subparagraph, point (d)
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
Article 16 TFEU

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 Article 5(1), first subparagraph, point (g), Article 5(1), first subparagraph, point (d) 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

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

Article 24 of the Charter and in the United Nations Convention on the Rights of the Child

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

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.

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

rticle 9(1) of Regulation (EU) 2016/679

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

Article 39 of the Charter,

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

Article 9(2), point (g) of Regulation (EU) 2016/679 and Article 10(2), point (g) of Regulation (EU) 2018/1725.

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

Article 16(2) of Regulation (EU) 2017/745

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

Article 13 of Directive (EU) 2016/680

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

Article 10 of Directive (EU) 2016/680
Article 4 (1) of Directive (EU) 2016/680

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 Article 4(3) of Directive (EU) 2019/790

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 Article 4(3) of Directive (EU) 2019/790

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 Article 2, point (1)(c), of Regulation (EU) Articles 5 and 6 of Regulation (EU) No 1025/2012

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 Article 54(3) of Regulation (EU) 2019/881

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 Unionshould 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 Article R23 of Annex I to Decision No 768/2008/EC

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 Article 16(6) of Regulation (EU) 2022/2065
Article 16(1) of that Regulation and should not influence the assessment and the decision on the illegality of the specific content

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 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)
Article 22(2), point (b) of Regulation (EU) 2016/679 and Article 24(2), point (b) of Regulation (EU) 2018/1725

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 Article 30 of Regulation (EU) 2019/1020. In accordance with Article 33 of that Regulation, 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 Article 9 of Regulation (EU) 2019/1020

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 Article 18 of Regulation (EU) 2019/1020

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 Article 261 TFEU. 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 Article 290 TFEU 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 Article 5 TEU. In accordance with the principle of proportionality as set out in that Article, this Regulation

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 Article 42(1) and (2) of Regulation (EU) 2018/1725 and delivered their joint opinion on 18 June 2021

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,