REGULATION ON A EUROPEAN APPROACH FOR ARTIFICIAL INTELLIGENCE

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

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

After consulting the Committee of the Regions[2],

Acting in accordance with the ordinary legislative procedure[3],

Whereas:

(1) Artificial intelligence is a fast evolving family of technologies that can contribute to a wide array of economic and societal benefits across the entire spectrum of industries and social activities. By improving prediction, optimising operations and resource allocation and personalizing service delivery, the use of artificial intelligence can provide key competitive advantages to companies and support socially and environmentally beneficial outcomes, for example in healthcare, farming, education, infrastructure management, energy, transport and logistics, public services, security, and climate change mitigation and adaptation, to name just a few.

(2) At the same time, some of the uses and applications of artificial intelligence may generate risks and cause harm to interests and rights that are protected by Union law. Such harm might be material or immaterial, insofar as it relates to the safety and health of persons, their property or other individual fundamental rights and interests protected by Union law.

(3) A legal framework setting up a European approach on artificial intelligence is needed to foster the development and uptake of artificial intelligence that meets a high level of protection of public interests, in particular the health, safety and fundamental rights and freedoms of persons as recognised and protected by Union law. This Regulation aims to improve the functioning of the internal market by creating the conditions for an ecosystem of trust regarding the placing on the market, putting into service and use of artificial intelligence in the Union.

[1] OJ [..]
[2] […]
[3] Position of the European Parliament of [..]

(4) In her political guidelines for the 2019-2024 Commission "A Union that strives for more"[4] President-elect von der Leyen announced the Commission would put forward legislation for a coordinated European approach on the human and ethical implications of artificial intelligence as well as a reflection on the better use of big data for innovation.

(5) Following up on that announcement, on 19 February 2020 the Commission published the White Paper on artificial intelligence - A European approach to excellence and trust,[5] with a view to setting out policy options on how to achieve the twin objective of promoting the uptake of artificial intelligence and of addressing the risks associated with certain uses of such technology and to launching a broad stakeholder consultation on such policy options. The consultation showed the great interest by stakeholders - including representatives from industry, academia, public authorities, international organisations, standardisation bodies, civil society organisations and citizens - in shaping the future EU regulatory approach to artificial intelligence. The great majority of stakeholders were supportive of regulatory intervention to address the challenges and concerns raised by artificial intelligence.

(6) Other European institutions repeatedly expressed calls for the European Commission to take legislative action to ensure a well-functioning internal market for AI systems where both benefits and risks of artificial intelligence are adequately addressed on EU level.

(7) In October 2020, the European Parliament adopted a number of resolutions related to artificial intelligence, including on ethics,[6] liability,[7] copyright,[8] artificial intelligence in criminal matters,[9] and artificial intelligence in education, culture and the audio-visual sector.[10] The European Parliament resolution on a framework of ethical aspects of artificial intelligence, robotics and related technologies specifically recommends to the Commission to propose a legislative action to harness the opportunities and benefits of artificial intelligence, but also to ensure protection of ethical principles. The resolution includes a text of the legislative proposal for a regulation on ethical principles for the development, deployment and use of artificial intelligence, robotics and related technologies.

(8) The European Council called for a "sense of urgency to address emerging trends" including "issues such as artificial intelligence […], while at the same time ensuring a high level of data

[4] Communication from President of the European Commission von der Leyen, A Union that strives for more, My agenda for Europe : political guidelines for the next European Commission 2019-2024, 2019.
[5] European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final, 2020.
[6] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).
[7] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence, 2020/2014(INL).
[8] European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies, 2020/2015(INI).
[9] European Parliament Draft Report, Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters, 2020/2016(INI).
[10] European Parliament Draft Report, Artificial intelligence in education, culture and the audiovisual sector, 2020/2017(INI).

protection, digital rights and ethical standards".[11] It also stated that the EU needs to be a global leader in the development of secure, trustworthy and ethical artificial intelligence, inviting the Commission to provide a clear, objective definition of high-risk AI systems.[12]

(9) The Council highlighted the importance of ensuring the full respect of the European citizen's rights by implementing ethics guidelines for the development and use of artificial intelligence within the European Union and at a global level and underlined that all EU legislation should be fit for the purpose and encourage the cross-border development and application of artificial intelligence-based technologies, and invited the Commission to take this objective into account when evaluating existing or considering new legislation.[13] The Presidency Conclusions also emphasized the increasing and largely positive effect of digital technologies on the daily lives of Europeans and called for addressing the challenges such as opacity, complexity, bias, a certain degree of unpredictability and partially autonomous behaviour of certain AI systems in order to ensure the compatibility of automated systems with fundamental rights and to facilitate the enforcement of legal rules.[14]

(10) Artificial intelligence should not be an end in itself, but a tool that has to serve people with the ultimate aim of increasing human well-being.[15] Rules for artificial intelligence available in the Union market or otherwise affecting Union citizens should thus put people at the centre (be human-centric), so that they can trust that the technology is used in a way that is safe and compliant with the law, including the respect of fundamental rights.

(11) At the same time, such rules for artificial intelligence should be balanced, proportionate and not unnecessarily constrain or hinder technological development. This is of particular importance because, although artificial intelligence is already present in many aspects of people's daily lives, it is not possible to anticipate all possible uses or applications thereof that may happen in the future.

(12) It is in the Union interest to preserve the EU's technological leadership and to ensure that Europeans can benefit from new technologies developed and functioning according to EU values and principles. The legal framework setting up a European approach on artificial intelligence should thus be robust and flexible at the same time. On the one hand, it should be comprehensive and future-proof in its fundamental regulatory choices and mechanisms. On the other hand, it should put in place a proportionate regulatory system centred on a well-defined risk-based regulatory approach, whereby legal intervention should be tailored to those concrete situations where there is a justified cause for concern or where such concern can reasonably be

[11] European Council, European Council meeting (19 October 2017) – Conclusion, EUCO 14/17, 2017, p. 7.

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

[13] Council of the European Union, Artificial intelligence b) Conclusions on the coordinated plan on artificial intelligence - Adoption, 6177/19, 2019.

[14] Council of the European Union, Presidency conclusions - The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change, 11481/20, 2020.

[15] European Commission, State of the Union Address by President von der Leyen at the European Parliament Plenary of 16 September 2020; COM(2020) SPEECH/20/1655; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Building Trust in Human-Centric AI, COM(2019) 168 final.

anticipated in the near future. At the same time, the legal framework should include flexible mechanisms that enable it to be dynamically adapted as the technology evolves and new concerning situations emerge.

(13) As a very powerful family of computer programming techniques that can be deployed in many fields of human activity for desirable uses, as well as more critical and harmful ones, there is no universally agreed definition of artificial intelligence. Nonetheless, for the purposes of this Regulation it is essential to introduce a definition that can stand the test of time while being able to provide to the addressees of this Regulation the legal certainty needed to enable compliance.

(14) A key tenet of the legal framework is that it should not focus on the technology as such. Instead, the legal framework should focus on the concrete utilisation of the technology in the form of AI systems (and the risks potentially deriving therefrom), intended as systems that can be used as a component of a product or on a stand-alone basis and whose outputs serve to partially or fully automate certain activities, including the provision of a service, the management of a process, the making of a decision or the taking of an action, irrespective of whether the AI system is developed and used by private or public organisations. As a component of a product, an AI system can be physically integrated into the product (embedded) or serve the functionality of the product without being integrated therein (non-embedded).

(15) The legal framework on artificial intelligence should be composed of the following building blocks: measures establishing a clearly defined risk-based approach; measures in support of innovation, measures facilitating the setting up of voluntary codes of conduct and a governance framework supporting the implementation of the Regulation at EU and national level and its adaptation as appropriate.

(16) In order to ensure a level playing field and an effective protection of EU citizen's rights and freedoms, the rules established by this Regulation should apply to providers of AI systems irrespective of whether they are established within the Union or in a third country outside the Union, to users of AI systems established within the Union and to providers and users of AI systems that are established in a third country outside the Union, to the extent the AI systems affect persons located in the Union. As appropriate, the Regulation should apply also to EU institutions, offices, bodies and agencies. AI systems exclusively used for the operation of weapons or other military purposes should be excluded from the scope of application of this Regulation.

(17) As a comprehensive legal framework for artificial intelligence and in order to ensure a consistent high level of protection of public interests, in particular the health, safety and fundamental rights and freedoms of persons, this Regulation should establish common normative standards for all high-risk AI systems. Nonetheless, in order to take account of the specificities of certain economic sectors, including the existence of particular governance and rule-making systems, the scope of application of this Regulation should be limited when it comes to AI systems intended to be used as safety components of products or systems, or which are themselves products or systems, covered by Regulation (EU) 2018/1139, Regulation (EU) 2018/858, Regulation (EU) 2019/2144, Regulation (EU) No 167/2013, Regulation (EU) No

168/2013, Directive (EU) 2016/797 and Directive (EU) 2016/798. In particular, as regards high-risk AI systems to be used in the aviation and railways sectors, the applicability of this Regulation should be limited to the requirements established in Chapter 1 Title III. As regards high-risk AI systems to be used in motor vehicles and marine equipment, the requirements established in Chapter 1 Title III should be taken into account by the Commission when adopting any relevant delegated or implementing acts according to any relevant legislation.

(18) In June 2018, the Commission appointed the High-Level Expert Group on Artificial Intelligence, which produced two deliverables: the Ethics Guidelines for Trustworthy AI and the Policy and Investment Recommendations for Trustworthy AI. In particular, in their first deliverable the High-Level Expert Group identified seven key requirements for Trustworthy AI, which were endorsed by the European Commission in its 2019 Communication "Building Trust in Human-Centric Artificial Intelligence".[16] The key requirements reflect a widespread and common approach, as evidenced by a plethora of ethical codes and principles developed by many private and public organisations in Europe and beyond, that artificial intelligence development and use should be guided by certain essential value-oriented principles. Depending on the jurisdiction, these principles may be already partially or fully embodied in legally enforceable provisions. For instance, in the Union the law on the protection of personal data and privacy already exhaustively materialises the principle of privacy, the EU law on consumer protection increases transparency for consumers and protects them from unfair commercial practices and the comprehensive EU product safety acquis already sets binding obligations in respect to the safety of products and devices.

(19) [Building upon the key requirements developed by the High-Level Expert Group and] in order to ensure that this Regulation introduces a proportionate yet effective set of binding legal provisions for AI systems, a clearly defined risk based approach should be followed. This implies the prohibition of certain artificial intelligence practices, the establishment of requirements and obligations for high-risk AI systems, whose compliance should be verified through ex-ante and ex-post enforcement tools, and the establishment of limited transparency obligations for certain other AI systems.

(20) It should be acknowledged that artificial intelligence can enable new manipulative, addictive, social control and indiscriminate surveillance practices that are particularly harmful and should be prohibited as contravening the Union values of respect for human dignity, freedom, democracy, the rule of law and respect for human rights.

(21) First, certain artificial intelligence-empowered practices have significant potential to manipulate natural persons, including through the automated adaptation of misleading user interfaces, and to exploit a person's vulnerabilities and special circumstances. Manipulative artificial intelligence practices should be prohibited when they cause a person to behave, form an opinion or take a decision to their detriment that they would not have taken otherwise.

[16] Human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; social and environmental well-being; accountability.

(22) Second, the use of artificial intelligence for the purposes of indiscriminate surveillance of natural persons should be prohibited when applied in a generalised manner to all persons without differentiation. The methods of surveillance could include monitoring and tracking of natural persons in digital or physical environments, as well as automated aggregation and analysis of personal data from various sources.

(23) Nonetheless, the artificial intelligence-empowered practices identified above shall be allowed when carried out by public authorities or on their behalf for the purpose of safeguarding public security and subject to appropriate safeguards for the rights and freedoms of third parties.

(24) Finally, algorithmic social scoring of natural persons should not be allowed if not carried out for a specific legitimate purpose of evaluation and classification, but in a generalised manner when the general purpose score is based on persons' behaviour in multiple contexts and/or personality characteristics and leads to detrimental treatment of persons which is either not related to the contexts in which the data was originally generated or collected, or disproportionate to the gravity of the behaviour. Detrimental treatment could occur for instance by taking decisions that can adversely affect and restrict the fundamental rights and freedoms of natural persons, including in the digital environment.

(25) High-risk AI systems may be placed on the Union market or otherwise put into service subject to compliance with mandatory requirements. This will ensure that high-risk AI systems available in the Union do not pose unacceptable risks to the protection of safety, fundamental rights or broader Union values and public interests.

(26) As regards high-risk AI systems that are safety components of products or systems, or which are themselves products or systems covered by Regulation (EU) 2018/1139, Directive (EU) 2016/797 and Directive (EU) 2016/798, the applicability of this Regulation shall be limited to the substantive provisions concerning mandatory requirements for high-risk AI systems.

(27) High-risk AI systems that are safety components of products or systems, or which are themselves products or systems covered by Regulation (EU) 2018/858 and Regulation (EU) 2019/2144, Regulation (EU) 167/2013 and Regulation (EU) 168/2013 do not fall within the scope of this Regulation. However, the Commission shall take into account the mandatory requirements for high-risk AI systems laid down in this Regulation, when adopting any relevant delegated or implementing acts.

(28) As regards AI systems intended to be used as a safety component of products which are covered by certain EU product safety legislation or AI systems which are devices in themselves in the meaning of Regulation (EU) 2017/745 of the European Parliament and of the Council[17]

[17] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance) (OJ L 117, 5.5.2017, p. 1–175).

and Regulation (EU) 2017/746 of the European Parliament and of the Council[18], it is appropriate to consider them high-risk if the product or device in question undergoes the conformity assessment procedure with a third-party conformity assessment body pursuant that relevant EU legislation.

(29) In particular, it should be considered as high-risk any AI system that is a safety component of machinery, radio equipment, toys… *[list of products to add]*.

(30) A classification of an AI system as high-risk for the purpose of this Regulation may not necessarily mean that the system as such or the product as a whole would necessarily be considered as 'high-risk' under the criteria of the sectoral legislation. This is notably the case for Regulation (EU) 2017/745, where a third-party conformity assessment is foreseen for medium-risk and high-risk products.

(31) As regards other (stand-alone) high-risk AI systems, two categories should be distinguished. A first category should include AI systems for the remote biometric identification of persons, around whose use in publicly accessible spaces there has been significant public concern, and AI systems that may primarily lead to adverse implications for personal safety. These AI systems should be subject to stricter conformity assessment procedures through the involvement of a notified body.

(32) For instance, AI systems intended to be used as safety components in the management and operation of essential public infrastructure networks should be considered high-risk as 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.

(33) The second category of (stand-alone) high-risk AI systems should be subject to conformity assessment through self-assessment by the provider. It is appropriate to classify as high-risk according to this category AI systems used to dispatch or establish priority in the dispatching of emergency first response services as they make decisions in very critical situations for the life and health of persons and their property.

(34) Similarly, AI systems used for determining access to educational and vocational training institutions or to evaluate persons on tests as part of or as a precondition for their education should be considered high-risk, as they may determine the educational and professional course of persons' lives and therefore affect their ability to secure their livelihood.

(35) Further, AI systems used in the recruitment, task allocation or evaluation of workers may appreciably impact workers' future career prospects and livelihood and should also be classified as high-risk. Working relationships may be characterised by a particular degree of dependency by workers. Throughout the recruitment process and in the evaluation, promotion, or retention of working relationships, such systems may perpetuate historical patterns of discrimination, for example against women, certain age groups, or persons of certain ethnic or racial origins. AI

[18] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (Text with EEA relevance) (OJ L 117, 5.5.2017, p. 176–332).

systems used to monitor the performance and behaviour of workers may also impact their rights to data protection and privacy.

(36) AI systems used to evaluate the creditworthiness of persons should be classified as high-risk as they determine said persons' access to financial resources and may therefore appreciably affect their course of life, for example if they deny them the opportunity to make certain investments. AI systems used for this purpose may also perpetuate historical patterns of discrimination in consumer finance, for example against persons of certain ethnic or racial origins or create new forms of discrimination.

(37) Persons applying for or receiving social security benefits and services from public authorities are [generally] dependent on these benefits and services and in a vulnerable position vis-à-vis the responsible authorities. If AI systems are used in determining whether such benefits and services should be denied, revoked or reclaimed by authorities, they may have an appreciable impact on persons' livelihood and may infringe their right to human dignity. They should therefore be considered high-risk.

(38) Actions by law enforcement, border control, the judiciary and authorities processing applications for asylum or visa may significantly impact persons' course of life and may interfere with their fundamental rights. In this context, persons are also particularly vulnerable and dependent on public authorities and certain harms may not be reversible. Therefore, AI systems should be considered high-risk if they are used in making decisions with a view to prevent, investigate, detect or prosecute a criminal offence or adopt other measures impacting on the personal freedom of an individual. This also applies if AI systems are used to determine the dispatch of law enforcement or border control officers in specific geographical areas. Further, AI systems used in the context of asylum and visa applications and for determining a person's eligibility to enter into the territory of the EU should be considered high-risk. Finally, AI systems should be considered high-risk if they are used to assist judges at court, unless for ancillary tasks.

(39) In order to ensure that the regulatory framework can be dynamically adapted to address potential harms caused by emerging ways in which artificial intelligence can be used, the Commission should be empowered to amend the list of high-risk AI systems through delegated acts. The list should be amended by the Commission based on an opinion by the European Artificial Intelligence Board. The Board should issue opinions based on an assessment report produced by a dedicated expert group on a request by the Board, if it identifies a potential need for an amendment to the list of high-risk AI systems.

(40) The classification of an AI system as high-risk should be based on its intended purpose - which should refer to the use for which an AI system is intended, including the specific context and conditions of use and - and be determined in two steps by considering whether it may cause certain harms and, if so, the severity of the possible harm and the probability of occurrence.

(41) The harms that may be caused by high-risk AI systems should include the injury or death of a person, damage of property, systemic adverse impacts for society at large, significant disruptions to the provision of essential services for the ordinary conduct of critical economic

and societal activities, adverse impact on financial, educational or professional opportunities of persons, adverse impact on the access to public services and any form of public assistance, and adverse impact on fundamental rights [as enshrined in the Charter]. [Fundamental rights potentially infringed due to the use of AI systems include the right to privacy and right to data protection, right not to be discriminated against, the freedoms of expression, assembly and association, personal freedom, right to property, right to an effective judicial remedy and a fair trial and right to international protection [asylum] [longer list of rights can be specified if necessary].]

(42) The ascertainment that AI systems may cause harm should be followed by an assessment of the severity of that harm and the probability of occurrence. In this context, account should be taken of a number of base-line criteria and a number of additional criteria. The base-line criteria shall always be taken into account in the assessment and shall include the extent of use of the AI system, the extent to which an AI system has caused harm or has given rise to significant concerns around the materialization of harm, the potential extent of the adverse impact of the harm, the potential of the AI system to scale and adversely impact a large number of persons, and the possibility that an AI system may generate more than one of the specifically defined harms. The additional criteria shall be taken into account as appropriate and relevant in consideration of the intended purpose of the AI system and shall include the extent to which potentially impacted persons are dependent on the outcome produced by an AI system, the extent to which they are in a vulnerable position vis-à-vis the user of an AI system, the degree of reversibility of the outcome produced by an AI system, the availability and effectiveness of legal remedies in Union and Member States law, and the extent to which existing Union legislation is able to prevent or substantially minimize the risks potentially produced by an AI system.

(43) Mandatory requirements concerning high-risk AI systems placed or otherwise put into service on the Union market should be complied with taking into account the intended purpose of the AI system and according to the risk management system to be established by the provider. Among other things, risk control management measures identified by the provider should be based on due consideration of the effects and possible interactions resulting from the combined application of the mandatory requirements and take into account the generally acknowledged state of the art, also including as reflected in relevant harmonised standards or common specifications.

(44) Requirements should be introduced as regards high-quality data sets, documentation and record-keeping, transparency and provision of information, human oversight, as well as robustness, accuracy and security.

(45) High data quality is essential for the performance of many AI systems, especially when techniques involving training of models are used. High quality training and testing data sets require the implementation of appropriate data governance and management practices. In order to ensure that an AI system performs as intended and risks to safety and fundamental rights are minimised, the training and testing data sets should be sufficiently relevant, representative, free of errors and complete in view of the intended purpose and should have the appropriate

statistical properties, including as regards the persons or groups of persons on which the high-risk AI system is intended to be used. As appropriate, training and testing data sets should take into account the features, characteristics or elements that are particular to the specific geographical and/or functional setting where the AI system is intended to be used. Particular attention should be provided to systems that continue to 'learn' after being placed on the market or put into service.

(46) For the development of artificial intelligence, it is necessary to ensure that various actors, such as providers of AI systems, notified bodies and other relevant entities, and digital hubs and testing experimentation facilities, can access and use high quality datasets to train, test, validate and assess conformity of AI systems. European common data spaces to be established by the Commission as part of its Data Strategy will be instrumental to provide trustful access to high quality data for this purpose. In health, for example, the European health data space will facilitate the access to health data and the training of AI algorithms on those datasets, in a privacy-preserving, secure, timely, transparent and trustworthy way, and with an appropriate institutional governance.

(47) Having information regarding the process how high-risk AI systems have been developed and how they perform throughout their lifecycle is essential to verify compliance with the requirements under this Regulation and other relevant Union and Member States legislation. This requires keeping records and the availability of certain technical documentation, such as on the general characteristics, capabilities and limitations of the system, algorithms, data, development, testing and validation processes used as well as documentation on the relevant risk management.

(48) To address the opacity that may make certain AI systems incomprehensible to natural persons or too complex, a certain degree of transparency of high-risk AI systems should be required. Users should be able to understand and control how the AI system outputs are produced. High-risk AI systems should thus be accompanied by relevant documentation and instructions of use and include concise, clear and, to the extent possible, non-technical information. This information should specify, in particular, the identity and contact details of the provider of the AI system, the capabilities and limitations of the AI system, its general logic and underlying assumptions, mitigating or precautionary measures, which shall be taken by users, and the expected lifetime of the AI system and any necessary maintenance and care measures.

(49) High-risk AI systems should be designed and developed in such a way that natural persons can oversee their functioning. For this purpose, appropriate technical and organisational measures should be identified by the provider before the placing on the market or putting into service of the AI system. Among others and as 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 operators, and that the natural persons to whom human oversight is assigned have the competence, the training and the authority necessary to carry out their role.

(50) High-risk AI systems should perform consistently throughout their lifecycle and meet a high level of accuracy, robustness and security. Also in light of the probabilistic nature of certain AI systems' outputs, the level of accuracy should be appropriate to the system's intended purpose and the AI system should indicate to users when the declared level of accuracy is not met so that appropriate measures can be taken by the latter. Robustness should imply that the system is resilient to errors, faults or inconsistencies that may occur within the system or in the environment in which the system operates, in particular due to their interaction with natural persons or software or hardware systems. The AI system should also be secure and resilient to attempts to alter its use or performance by malicious third parties intending to exploit the system's vulnerabilities.

(51) The rules applicable to the placing on the market, putting into service and use of high-risk AI systems should be aligned, where appropriate, with the New Legislative Framework for the Marketing of Products, which consists of Regulation (EC) No 765/2008 of the European Parliament and of the Council[19] setting out the requirements for accreditation and the market surveillance of products, Decision No 768/2008/EC of the European Parliament and of the Council[20] on a common framework for the marketing of products. [and Regulation (EU) 2019/1020 of the European Parliament and of the Council[21] on market surveillance and compliance of products].

(52) In line with New Legislative Framework principles, it is appropriate that a specific natural or legal person or public body or agency, defined as the provider, should take the responsibility for the placing on the market or putting into service of a high-risk AI system, regardless of whether that natural or legal person or public body or agency is the person who designed or developed the system.

(53) The provider should be responsible for ensuring the compliance of high-risk AI systems with the requirements of this Regulation. In this context, they should inter alia establish a sound quality management system, ensure the accomplishment of the requirement conformity assessment procedure, draw up the relevant documentation and establish a robust post-market monitoring system.

(54) Based on the principles of the EU product legislation, a unique and identifiable economic operator must hold the legal responsibility for the finished product as a whole. For this reason, where a high-risk AI system is not placed on the market or put into service independently in a final product which is covered under a relevant New Legislative Framework sectorial legislation and for which this Regulation applies, the manufacturer of the final product as

[19] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

[20] Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (OJ L 218, 13.8.2008, p. 82).

[21] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (Text with EEA relevance) (OJ L 169, 25.6.2019, p. 1–44).

defined under the relevant New Legislative Framework legislation should comply with the obligations of the provider established in this Regulation and notably ensure that the AI system in the final product complies with the requirements of this Regulation.

(55) For providers who are not established in the Union, the authorised representative should play a role in ensuring the compliance of the AI systems placed on the market or put into service by those providers and in serving as their contact person established in the Union.

(56) In line with New Legislative Framework principles, specific obligations for relevant economic operators, such as importers and distributors, should be set to ensure legal certainty and facilitate regulatory compliance by those relevant operators.

(57) Given the nature of AI systems and the key role that the use thereof plays in respect of risks to safety and fundamental rights, including as regard the need to ensure proper monitoring of the performance of an AI system in a real-life setting, it is also appropriate to set specific responsibilities for users. Users should in particular use high-risk AI systems in accordance with the instructions of use and take all technical and organisational measures indicated by the providers to address residual risks posed by the use of AI systems. Furthermore, users have certain obligations with regards to monitoring for evident anomalies or irregularities and with regards to record-keeping of the input data.

(58) In the light of the complexity of the artificial intelligence value chain, it is appropriate to set certain obligations for all relevant third parties, notably the ones involved in sale and supply of software, software tools and components, pre-trained models and data. In particular, they should cooperate with providers and users to enable their compliance with the obligations under this Regulation.

(59) Standardisation should play a key role to provide technical solutions to providers to ensure compliance with this Regulation. Compliance with harmonised standards as defined in Regulation (EU) No 1025/2012 of the European Parliament and of the Council[22] should be a means for providers to demonstrate conformity with the requirements of this Regulation. However, the Commission could adopt common technical specifications in areas where no harmonised standards exist or where they are insufficient.

(60) 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. Given the more extensive experience of professional pre-market certifiers in the field of product safety and the different nature of risks involved, it is appropriate that a third-party intervention in the conformity assessment is foreseen only where high-risk AI systems might primarily affect negatively the health and safety of persons. For other high-risk AI systems, as a matter of principle the conformity assessment should be carried out by the provider under

[22] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (Text with EEA relevance) (OJ L 316, 14.11.2012, p. 12–33).

their own responsibility. [This approach should however be specifically reviewed after XX years following the entry into application of the Regulation in light of relevant developments.]

(61) In order to avoid an excessive burden on notified bodies, especially in the early period of application of this Regulation, and to ensure that they intervene only when necessary, where harmonised standards exist and are applied by providers, the involvement of a third-party in the conformity assessment would not be mandatorily required.

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

(63) In order to carry out third-party conformity assessment for certain high-risk AI systems other than those covered by relevant existing EU sectorial New Legislative Framework legislations, notified bodies should be designated under this Regulation by the national competent authorities, provided they are compliant with a set of requirements, notably on independence, competence and absence of conflicts of interests. Notified bodies should be continuously monitored by national competent authorities. Notified bodies should verify that the relevant high-risk AI systems are compliant with this Regulation.

(64) It is appropriate that an AI system undergoes a new conformity assessment whenever a change occurs which may affect the compliance of the system with this Regulation or when the intended purpose of the system changes. For AI systems which continue to 'learn' after being placed on the market or put into service (i.e. they automatically adapt how functions are carried out) changes to the algorithm and performance which have not been pre-determined and assessed at the moment of the conformity assessment shall result in a new conformity assessment of the AI system.

(65) High-risk AI systems should bear the CE marking to indicate their conformity with this Regulation so that they can move freely within the Union. Member States should not create obstacles to the placing on the market or putting into service of AI systems that comply with the requirements laid down in this Regulation.

(66) As the COVID-19 crisis has clearly shown, under certain conditions, rapid availability of innovative technologies may be crucial for health and safety of persons 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 and the protection of industrial and commercial property, Member States could authorise the placing on the market or putting into service of AI systems which have not undergone a conformity assessment.

(67) In order to facilitate the work of the Commission and the Member States in the artificial intelligence field as well as to increase the transparency vis-à-vis the public, providers should

be required to register their high-risk AI system in the EU database, to be established and managed by the Commission. The Commission should be the controller of that database, in the meaning of the General Data Protection Regulation (EU) 2016/679 (GDPR). In order to ensure the full functionality of the database, when deployed, the procedure for setting the database should include the elaboration of functional specifications by the Commission and an independent audit report.

(68) 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. In particular, natural persons should be notified that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use. Moreover, users, who use an AI system to generate or manipulate image, audio or video content that appreciably resembles existing persons, places or events and would falsely appear to a reasonable person to be authentic, should disclose that the content has been artificially created or manipulated by labelling the artificial intelligence output accordingly and disclosing its artificial origin. This labelling obligation should not apply where the use of such content is necessary for the purposes of safeguarding public security or for the exercise of a legitimate right or freedom of a person such as for satire, parody or freedom of arts and sciences and subject to appropriate safeguards for the rights and freedoms of third parties.

(69) Biometric identification means that a person's biometric data is compared to a reference database to find out if the person's biometric data is stored there. Such reference data base could be based on a specific watch list of person and a biometric identification system could be used both in limited and restricted settings or in wide settings, where the identification of persons can happen at a distance (remote biometric identification).

(70) The use of remote biometric identification systems in publicly accessible spaces bears specific challenges for the protection of fundamental rights and freedoms, including human dignity, respect for private and family life, protection of personal data and non-discrimination. For example, the placement in publicly accessible spaces can impact the behaviour of persons in public and bears the risk of deterring persons from exercising democratic freedoms, including the freedom of expression, association and assembly. Moreover, technical inaccuracies can lead to biased results and entail discriminatory effects. This is particularly relevant when it comes to age, ethnicity, sex or disabilities.

(71) These forms of remote biometric identification systems have raised important societal concerns. A large majority of respondents in the public consultation following the publication of the White Paper on Artificial Intelligence favoured a ban of the use of remote biometric identification systems in public spaces, the introduction of a specific EU guideline or legislation, or other limits to the use of remote biometric identification in public spaces.

(72) Considering the risks emerging from the use of remote biometric identification in publicly accessible spaces, it is appropriate to consider such AI systems to be high-risk AI systems. The sensitive nature of biometric data is recognised in the EU data protection rules, which make

such data subject to special protection: the processing of biometric data is prohibited in principle - but there are a limited number of conditions under which such processing can be lawful. A Data Protection Impact Assessment is required for the processing of biometric data on a large scale for the purpose of uniquely identifying a natural person, to be carried out by the data controller.

(73) In addition to the conformity assessment required for high-risk systems under this Regulation and building on the Data Protection Impact Assessment, the use of remote biometric identification in publicly accessible spaces should be subject to an authorisation procedure that addresses the specific risks implied by the use of the technology. The authorisation procedure should take account of the Data Protection Impact Assessment. Furthermore the authorising authority should consider in its assessment the likelihood and severity of harm caused by inaccuracies of a system used for a given purpose, in particular with regard to age, ethnicity, sex or disabilities. It should further consider the societal impact, considering in particular democratic and civic participation, as well as the methodology, necessity and proportionality for the inclusion of persons in the reference database.

(74) In order to ensure the consistency of enforcement of this Regulation with the data protection rules, authorising authorities should be the supervisory authorities entrusted under the data protection rules with the assessment of the Data Protection Impact Assessment. In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, a close cooperation between authorising authorities, the European Data Protection Board and the European Artificial Intelligence Board is required.

(75) Artificial intelligence is a rapidly developing family of technologies that requires novel forms of regulatory oversight and a safe space for experimentation, while ensuring responsible innovation and integration of appropriate safeguards and risk mitigation measures. To ensure a legal framework that is innovation-friendly, future-proof and resilient to disruption, national competent authorities from one or more Member States should be encouraged to establish artificial intelligence regulatory sandboxing schemes 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.

(76) [The objectives of the regulatory sandboxing schemes shall be to foster artificial intelligence innovation by establishing a controlled incubation and testing environment, while integrating appropriate protections and safeguards in compliance with relevant Union and Member States legislation; to enhance legal certainty for companies and the national competent authorities' oversight and understanding of the opportunities, emerging risks and the impacts of artificial intelligence use, and to accelerate access to markets, including by removing barriers for Small and Medium Enterprises (SMEs) and start-ups.]

(77) Within the framework of the regulatory sandboxes, cooperation between the competent authorities designated under this Regulation and under other sectoral legislation is key where multiple legal frameworks are applicable to AI systems' development and use. These competent authorities shall be empowered to exercise their discretionary powers and levers of proportionality in relation to artificial intelligence projects of entities participating the sandbox,

while fully preserving authorities' supervisory and corrective powers. Coordination between the various sandboxing schemes shall be ensured within the framework of the European Artificial Intelligence Board with a view to fostering a common European approach to artificial intelligence innovation. To reduce the regulatory burden on SMEs and start-ups for compliance with this Regulation, it is appropriate that competent authorities, notified bodies, Digital Hubs and Testing Experimentation Facilities envisage specific supporting measures, including by taking into the account the special needs of SMEs, providing priority access and privileged condition for participation and provision of dedicated information, training and other services.

(78) In order to facilitate a smooth, effective and harmonised implementation of this Regulation a European Artificial Intelligence Board should be established. The Board should be composed of one representative per Member State and a representative [respectively] of the European Commission [and the European Data Protection Supervisor]. The Board will be responsible for a number of tasks, including for issuing relevant recommendations and opinions to the Commission, with regard to the list of prohibited artificial intelligence practices and the list of high-risk AI systems. The Board should carry out its tasks in close cooperation with other relevant bodies and structures established at EU level, including the European Data Protection Board, the EU network of market surveillance as well as other sectoral bodies and authorities at EU level [e.g. the European Banking Authority]. Such cooperation should be without prejudice to the independence and the powers granted by Union law to the Board and any other authority or body established at EU level. The Board should also exchange on a regular basis with stakeholders such as civil society organisations, businesses and industry associations, social partners and academia, and ensure that their opinions and views can inform its activities to an appropriate extent.

(79) Given the technical nature of many of the deliverables expected from the European Artificial Intelligence Board, the Board should benefit from the expertise and the technical and scientific advice of a group of independent experts. To facilitate the full involvement of the experts, they should be remunerated for their preparatory work and participation in the meetings.

(80) 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 and notified bodies with their obligations under this Regulation, Digital Innovation Hubs and Testing Experimentation Facilities established in accordance with [link to DEP] should play a role in the implementation of this Regulation. They should in particular provide technical and scientific advice and testing facilities in accordance with operational procedures to be set out by the Commission in an implementing act.

(81) It is appropriate that the Commission facilitates, to the extent possible, access to testing experimentation facilities to bodies, groups or laboratories established or accredited pursuant to any relevant Union harmonisation legislation and which fulfil tasks concerning in the context of conformity assessment of products or devices covered by that Union harmonisation legislation. This is notably the case for expert panels, expert laboratories and reference

laboratories in the field of medical devices pursuant to Regulation (EU) 745/2017 and Regulation (EU) 746/2017.

(82) Member States hold a key role in the application and enforcement of this Regulation. In this respect, each Member State should designate one or more national competent authorities, for the purpose of supervising the application and implementation of this Regulation, or parts thereof. In order to increase organisation efficiency on the side of Member States and to set an official point of contact vis-à-vis the public and other counterparts at Member State and EU levels, in each Member State, one national authority should be designated as national supervisory authority.

(83) In order to ensure that experience from the use of high-risk AI systems they design and develop is taken into account for improving the development process or take any possible corrective action in a timely manner, all providers should have a post-market monitoring system in place. 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 any serious incidents or breaches to national and EU law protecting fundamental rights resulting from the use of their AI systems.

(84) In order to ensure that enforcement of this Regulation is appropriate and effective, market surveillance activities, including checks and inspections, should be carried out by market surveillance authorities, without prejudice to the supervisory activities of other competent authorities such as Data Protection Authorities. It is appropriate that the market surveillance system in this Regulation builds on Regulation (EU) 2019/1020, which shall apply.

(85) The development of AI systems other than high-risk AI systems in line with requirements of this Regulation may lead to a larger uptake of trustworthy AI in the Union. Providers of non high-risk AI systems should be encouraged by the Commission to create codes of conduct intended to foster the voluntary application of the mandatory requirements applicable to high-risk AI systems. Codes of conduct may cover one or more AI systems and should include technical specifications to ensure compliance. They may further provide for voluntary commitments to meet additional requirements related, for example, to environmental sustainability, accessibility to persons with disability, stakeholders' participation in the design and development of AI systems, and diversity of the development teams. Such codes of conduct may be proposed for approval by the Commission with a view to achieving an EU-wide scope of application. Member States shall monitor compliance by providers with the approved codes.

(86) In order to ensure trustful and constructive cooperation of competent authorities on EU and national level, all parties involved in the application of this Regulation shall respect the confidentiality of information and data obtained in carrying out their tasks.

(87) 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. For certain specific infringements, Member States should take into account the margins and criteria set out in this Regulation.

(88) In order to swiftly take account and respond to developments as regards the technology, emerging forms of use of artificial intelligence and possibly associated risks, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission to amend or further specify the lists on approaches and technologies in Annex I, high-risk AI systems in Annex II, EU harmonisation legislation in Annex III and elements of technical documentation in Annex IV, as well as to update the content of the EU declaration of conformity in Annex V and the conformity assessment procedure in Annex VI.

(89) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011.[23]

(90) The examination procedure should be used for the adoption of implementing acts on the adoption of common specifications; definition of modalities for the operation of an artificial intelligence sandboxing scheme; structure of fees and recoverable costs for the services provided by Digital Hubs and Testing Experimentation Facilities and request to the Member States to implement corrective acts towards a notified body. [and determination of the operational aspects related to the tasks to be carried out by Digital Hubs and Testing Experimentation Facilities in the context of this Regulation.]

(91) Since the objective of this Regulation, namely creating the conditions for an ecosystem of trust regarding the placing on the market, putting into service and use of artificial intelligence in the Union, 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 of the Treaty on European Union. 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.

(92) Given the need to ensure that the infrastructure related to the governance and the operation of the conformity assessment is operational by the time this Regulation is applicable, the provisions on Notified Bodies and governance structure should apply at an earlier date than the general date of application of this Regulation.

[Recitals to be double checked/fine-tuned after Articles have been defined]

[23] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p.13).

TITLE I

GENERAL PROVISIONS

Article 1

Subject matter and objective

1. This Regulation lays down harmonised rules concerning the placing on the market, putting into service and use of high-risk AI systems in the Union. It also lays down harmonised transparency rules for AI systems intended to interact with natural persons and AI systems used to generate or manipulate image, audio or video content.

2. This Regulation aims to improve the functioning of the internal market by creating the conditions for the uptake of artificial intelligence that is compatible with Union law and values and contributes to a high level of protection of health and safety and the fundamental rights and freedoms of persons.

Article 2

Scope

1. This Regulation shall apply to the placing on the market, putting into service and use of AI systems defined in Article 3(2).

2. This Regulation applies to:

(a) providers placing on the market or putting into service AI systems in the Union, irrespective of whether they are established within the Union or in a third country outside the Union;
(b) users of AI systems established within the Union;
(c) providers and users of AI systems that are established in a third country outside the Union, to the extent the AI systems affect persons located in the Union;
(d) EU institutions, offices, bodies and agencies when falling within one of the categories (a) or (b) above.

3. With regard to high-risk AI systems referred to in Article 5(2), this Regulation shall apply as follows:

(a) for high-risk AI systems that are safety components of products or systems, or which are themselves products or systems, covered by Regulation (EU) 2018/1139 of the European Parliament and of the Council[24], Directive (EU) 2016/797 of the European

[24] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (Text with EEA relevance) (OJ L 212, 22.8.2018, p. 1–122).

Parliament and of the Council[25] and Directive (EU) 2016/798 of the European Parliament and of the Council[26], the applicability of this Regulation is limited to Chapter 1 Title III; *[Empowerment for implementing act TBD]*

(b) for high-risk AI systems that are safety components of products or systems, or which are themselves products or systems, covered by Regulation (EU) 2018/858 of the European Parliament and of the Council[27] and Regulation (EU) 2019/2144 of the European Parliament and of the Council[28], Regulation (EU) 167/2013 of the European Parliament and of the Council[29], Regulation (EU) 168/2013 of the European Parliament and of the Council[30] the requirements of this Regulation set out in Chapter 1, Title III shall be taken into account by the Commission when adopting any relevant delegated acts in accordance with Article 53 of Regulation (EU) 2018/858, any relevant implementing act in accordance with Article 11 of Regulation (EU) 2019/2144, any relevant delegated act in accordance with Article 17(4) of Regulation (EU) 167/2013 and any relevant delegated act in accordance with Article 22(5) of Regulation (EU) 168/2013;

(c) for high-risk AI systems that are safety components of marine equipment, or that are themselves marine equipment, covered by Directive 2014/90/EU, the requirements of this Regulation set out in Chapter 1, Title IV shall be taken into account by the Commission when carrying out its activities pursuant to Article 8(1) of Directive 2014/90/EU.

4. This Regulation does not apply to AI systems exclusively used for the operation of weapons or other military purposes.

[25] Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (Text with EEA relevance) (OJ L 138, 26.5.2016, p. 44–101).

[26] Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety (Text with EEA relevance) (OJ L 138, 26.5.2016, p. 102–149).

[27] Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (Text with EEA relevance) (OJ L 151, 14.6.2018, p. 1–218).

[28] Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (Text with EEA relevance) (OJ L 325, 16.12.2019, p. 1–40).

[29] Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles (Text with EEA relevance) (OJ L 60, 2.3.2013, p. 1–51).

[30] Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles (Text with EEA relevance) (OJ L 60, 2.3.2013, p. 52–128).

5. This Regulation is without prejudice to the competences of the Member States regarding activities that fall outside the scope of Union law.

Article 3

Definitions

1. For the purpose of this Regulation, the following definitions shall apply:

(1) 'artificial intelligence system or AI system' means software that is developed with one or more of the approaches and techniques listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy. An AI system can be used as a component of a product, also when not embedded therein, or on a stand-alone basis and its outputs may serve to partially or fully automate certain activities, including the provision of a service, the management of a process, the making of a decision or the taking of an action;

(2) 'provider of an AI system' means a natural or legal person, public authority, agency or other body who develops an AI system or has it developed and places it on the market under its own name or trademark or puts it into service under its own name or trademark or for its own use, whether for payment or free of charge;

(3) 'user' means any natural or legal person, public authority, agency or other body under whose authority and responsibility the AI system is used, except where the use is in the course of a personal or transient activity;

(4) ['small-scale user' means any user that is a self-employed person or an individual professional and a micro-enterprise within the meaning of Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.[31]]

(5) 'authorised representative' means any natural or legal person established in the Union who has received a written mandate from a provider of an AI system to perform on their behalf obligations and procedures established by this Regulation;

(6) 'importer' means any natural or legal person established within the Union that places on the market an AI system that bears the name or trademark of a person established outside the Union;

(7) 'distributor' means any natural or legal person other than the provider and the importer in the supply chain that makes an AI system available on the Union market without affecting its properties;

(8) 'placing on the market' means the first making available of an AI system on the Union market;

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

[31] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C (2003) 1422) (OJ L 124, 20.5. 2003, p. 36).

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

(11) ‘intended purpose’ means the use for which an AI system is intended by the provider, including the specific context and conditions of use, according to the information supplied by the provider of the AI system in the instructions for use, promotional or sales materials and statements, and as indicated by the provider of the AI system in the technical documentation pursuant to Annex IV;

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

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

(14) ‘instructions for use’ means the information provided by the provider to inform the user of an AI system's intended purpose and proper use and of any precautions to be taken;

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

(16) ‘withdrawal of an AI system’ means any measure aimed at preventing the distribution, display and offer of an AI system that is not compliant with the requirements under this Regulation;

(17) ‘performance of an AI system’ means the ability of an AI system to achieve its intended purpose as stated by the provider;

(18) ‘conformity assessment’ means the process demonstrating whether the requirements of this Regulation relating to an AI system have been fulfilled;

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

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

(21) ‘substantial modification’ means a change made or occurring to the AI system following its placing on the market or putting into service which may affect the compliance of the AI system with this Regulation or result in a modification to the intended purpose for which the AI system has been assessed;

(22) ‘CE marking of conformity’ or ‘CE marking’ means a marking by which a provider indicates that an AI system is in conformity with the applicable requirements set out in this Regulation and other applicable Union harmonisation legislation providing for its affixing;

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

(24) ‘market surveillance authorities’ means the national competent authorities carrying out the activities and measures pursuant to Regulation (EU) 2019/1020 on market surveillance and compliance of products to check and ensure that AI systems comply with the requirements set out in the relevant Union harmonisation legislation and do not endanger health, safety, fundamental rights and Union values or any other aspect of public interest protection;

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

(26) ‘common specifications’ means a set of technical or other requirements, other than a standard, that provides a means of complying with the legal obligations under this Regulation;

(27) ‘emotional recognition system’ means an automated system for the purpose of identifying or inferring emotions or intentions of persons on the basis of their personal data;

(28) ‘categorisation system’ means an automated system for the purpose of predicting on the basis of their personal data the affiliation of persons to specific categories, such as sex, age, ethnic origin or sexual orientation;

(29) ‘biometric data’ means personal data as defined in Article 4(14) of Regulation (EU) 2016/679;

(30) ‘remote biometric identification system’ refers to an automated system for the purpose of the identification of persons at a distance on the basis of their biometric data. A person is identified when the template of their biometric data is matched with a template already stored in a reference database;

(31) ‘publicly accessible space‘ means any place open to the public;

(32) ‘national supervisory authority’ means the public authority to which a Member State assigns the responsibility for the overall implementation and application of the Regulation, for coordinating the activities of other national competent authorities and for acting as the single contact point for the Commission and the European Artificial Intelligence Board;

(33) ‘national competent authority’ means the public body to which a Member State assigns the responsibility to carry out certain activities related to the implementation and application of this Regulation;

(34) ‘AI regulatory sandbox’ means a controlled incubation and live-testing environment established under the strict oversight of the relevant national competent authorities which shall facilitate supervised development, testing and validation of innovative AI systems, while ensuring compliance with this Regulation and other applicable Union and Member States legislation.

(35) ‘serious incident’ means any incident that directly or indirectly leads, might have led or might lead to any of the following: (a) the death of a person or serious damage to a person’s health or property, (b) a serious and irreversible disruption of critical public utilities or assets;

(36) ‘breach of an obligation under Union or Member States law intended to protect fundamental rights’ means a breach of a primary or secondary law obligation that adversely affects one or more fundamental rights of a person, where such rights are

protected by the Charter, under Union law or when Member States are implementing Union law giving effect to such rights.

2. The Commission is empowered to adopt delegated acts in accordance with Article 64 to specify technical elements of the definitions laid down in paragraph 1, including Annex I, and to update those definitions to market and technological developments.

TITLE II

PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES

Article 4

1. The following list of artificial intelligence practices are prohibited as contravening the Union values or violating fundamental rights protected under Union law:

(a) AI systems designed or used in a manner that manipulates human behaviour, opinions or decisions through choice architectures or other elements of user interfaces, causing a person to behave, form an opinion or take a decision to their detriment.
(b) AI systems designed or used in a manner that exploits information or prediction about a person or group of persons in order to target their vulnerabilities or special circumstances, causing a person to behave, form an opinion or take a decision to their detriment.
(c) AI systems used for indiscriminate surveillance applied in a generalised manner to all natural persons without differentiation. The methods of surveillance may include large scale use of AI systems for monitoring or tracking of natural persons through direct interception or gaining access to communication, location, meta data or other personal data collected in digital and/or physical environments or through automated aggregation and analysis of such data from various sources.
(d) AI systems used for general purpose social scoring of natural persons, including online. General purpose social scoring consists in the large scale evaluation or classification of the trustworthiness of natural persons [over certain period of time] based on their social behaviour in multiple contexts and/or known or predicted personality characteristics, with the social score leading to:
    (i) a systematic detrimental treatment of certain natural persons or whole groups thereof in social contexts not related to the contexts in which the data was originally generated or collected; or
    (ii) detrimental treatment of certain natural persons or whole groups thereof that is disproportionate to the gravity of their social behaviour.

2. The prohibition under paragraph 1, point (a), (b) and (c) shall not apply when such practices are authorised by law and are carried out [by public authorities or on behalf of public

authorities] in order to safeguard public security and are subject to appropriate safeguards for the rights and freedoms of third parties in compliance with Union law.

TITLE III

HIGH-RISK AI SYSTEMS

Article 5

High-risk AI systems

1. AI systems intended to be used as safety components of products, or which are themselves products, covered by, the Union harmonisation legislation listed in Annex III shall be classified as high-risk, irrespective of whether they are placed on the market independently from the product or not, if the product in question undergoes the conformity assessment system with a third-party conformity assessment body pursuant to that relevant Union harmonisation legislation. Where, in accordance with that relevant Union harmonisation legislation, the product in question does not undergo a conformity assessment system with a third-party conformity assessment body because the manufacturer has applied all harmonised standards in full, those harmonised standards shall also cover all the applicable requirements of this Regulation as listed in Title III

2. AI systems intended to be used as safety components of products, systems or equipment, or which are themselves products, systems or equipment, covered by Regulation (EU) 2018/1139, Regulation (EU) 2018/858, Regulation (EU) 2019/2144, Regulation (EU) No 167/2013, Regulation (EU) No 168/2013, Directive (EU) 2016/797, Directive (EU) 2016/798 and Directive 2014/90/EU shall be classified as high-risk.

3. Annex II contains the list of AI systems other than those referred to in paragraph 1 and 2 that shall be classified as high-risk.

Article 6

Updating of high-risk AI systems

1. The Commission is empowered to adopt delegated acts in accordance with Article 64 to update the list in Annex II by adding new high-risk AI systems, where it has identified that other AI systems generate a high level of risk of harm in the same way as the high-risk AI systems already listed in Annex II.

2. An AI system shall be considered to generate a high level of risk of harm pursuant to the provisions of paragraphs 3 to 6 of this Article.

3. The harm shall be any of the following:

(a) injury or death of a person, damage of property;
(b) systemic adverse impacts for society at large, including by endangering the functioning of democratic processes and institutions and the civic discourse, the environment, public health, [public security];
(c) significant disruptions to the provision of essential services for the ordinary conduct of critical economic and societal activities;
(d) adverse impact on financial[economic], educational or professional opportunities of persons;
(e) adverse impact on the access by a person or group of persons to public services and any form of public assistance;
(f) adverse impact on fundamental rights [as enshrined in the Charter], in particular on the right to privacy, right to data protection, right not to be discriminated against, the freedoms of expression, assembly and association, personal freedom, right to property, right to an effective judicial remedy and a fair trial and right to international protection [asylum] [*longer list of rights can be specified if necessary*]

4. The high level of risk shall result from both the [degree of] severity of the possible harm and the [degree of] probability of occurrence of the same. *[**OPTIONAL**: The determination of a high level of risk may result from different combinations of the degrees of severity and degrees of probability. The Commission shall, through implementing acts in accordance with the examination procedure referred to in Article 65(2), lay out detailed provisions for a risk assessment scheme, notably provisions establishing the degrees of severity and probability, the combinations of degrees of severity and probability that would result in a high level of risk and a methodology for assessing the degrees of severity and probability.]*

5. The severity of harm and the probability of its occurrence shall be determined on the basis of the criteria listed in this paragraph. The criteria listed in point (a) shall always be taken into account (base-line criteria). The criteria listed in point (b) shall be taken into account as appropriate and relevant in consideration of the intended purpose of the AI system (additional criteria).

(a) Base-line criteria:
  (i) the extent to which an AI system has been used or is about to be used, provided that the AI system is used or is about to be used, at a minimum, in three or more Member States;
  (ii) the extent to which an AI system has caused any of the harms referred to in paragraph 4 or has given rise to significant concerns around the materialization of the same harms, as emerging from reports or documented allegations submitted to national competent authorities;
  (iii) the potential extent of the adverse impact of the harm as defined in paragraph 4;
  (iv) the potential of the AI system to be used at scale and adversely impact a large number of persons *[quantitative metric such as 1/20 of EU population or other]* or entire groups of persons based on characteristics such as race, sex, sexual orientation, nationality, ethnic origin, profession, political opinions, religious or philosophical beliefs;

(v) the possibility that an AI system may generate more than one of the harms referred to in paragraph 4.

(b) Additional criteria:

(i) the extent to which potentially adversely impacted persons are dependent on the outcome produced by an AI system, notably because it is not factually or legally possible to opt-out from that outcome;

(ii) the extent to which potentially adversely impacted persons are in a vulnerable position vis-à-vis the user of an AI system, notably due to an imbalance of power, knowledge, economic, social or cultural conditions,

(iii) the extent to which the outcome produced by an AI system is easily or readily reversible, provided that outcomes having an impact on the health and safety of persons shall be considered as not easily or readily reversible;

(iv) the availability and effectiveness of legal remedies in Union and Member States law;

(v) the extent to which existing Union legislation is able to prevent or substantially minimize the risks potentially produced by an AI system;

(vi) *[**OPTIONAL**: the prevalence and effectiveness of specific risk management or quality assurance processes in specific economic sectors or areas of activity that are able to prevent or substantially minimise the risks potentially produced by an AI system]*.

7. Before adopting the delegated acts according to paragraph 1 of this Article, the Commission shall seek the opinion of the Board pursuant to the provisions of Article 48(2) and seek feedback from relevant stakeholders through a public consultation.

8. The Commission is empowered to adopt delegated acts in accordance with Article 64 to update the list of the Union harmonisation legislation listed in Annex III and Union legislation referred to in paragraph 2 of this Article.

Chapter 1

REQUIREMENTS FOR HIGH-RISK AI SYSTEMS

Article 7

Compliance with the requirements

1. High-risk AI systems shall be compliant with the requirements established in this Title. Compliance with the requirements shall be ensured taking into account the intended purpose of the high-risk AI systems and according to the risk management system referred to in Annex VIII.

2. Compliance with the requirements shall be assessed before the placement of high-risk AI systems on the market or their putting into service via the conformity assessment procedures established in Chapter 4 of this Title.

Article 8

Data sets

1. High-risk AI systems which make use of techniques involving the training of models with data shall be developed on the basis of training and testing data sets that are of high quality pursuant to the provisions of this Article.

2. High quality data sets shall ensure that the high-risk AI system performs as intended and:

(a) does not incorporate any intentional or unintentional biases, which may become the source of discriminatory impacts prohibited by Union and Member State law once the high-risk AI system is used according to its intended purpose;
(b) does not produce unintended [adverse] outcomes under conditions of reasonably foreseeable misuse.

3. Training and testing data sets shall be subject to appropriate data governance and management practices, including as regards relevant design choices. Among others, these practices shall relate to data collection, relevant data preparation processing operations such as annotation, labelling, cleaning, enrichment and aggregation, and the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent. These practices shall also include a prior assessment of the availability, quantity and suitability of the data sets that would be needed, the identification of any possible data gaps or shortcomings and how these can be addressed.

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

5. Training and testing data sets shall take into account the features, characteristics or elements that are particular to the specific geographical, behavioural or functional setting where the high-risk AI system is intended to be used.

6. High-risk AI systems that continue to 'learn' after being placed on the market or put into service shall be developed in such a way to ensure that possibly biased outputs due to feedback loops are duly addressed with appropriate mitigation measures and to ensure that no changes are integrated to the high-risk AI system and its performance which have not been pre-determined at the moment of the initial conformity assessment of the high-risk AI system and, where applicable, of the product of which it is a component.

7. High-risk AI systems shall not be tested on data sets that have already been used in full or in part for the training of the same high-risk AI systems.

8. To the extent it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the processing of special categories of personal data shall be deemed a reason of substantial public interest according to Article 9(2)(g)

of Regulation (EU) 2016/679, subject to appropriate safeguards for the fundamental rights and freedoms of persons, including technical limitations of the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation and encryption, where anonymisation may significantly affect the purpose pursued.

9. Appropriate data governance and management practices shall apply also for the development of high-risk AI systems other than those referred to in paragraph 1 in order to ensure that these comply with the provisions of paragraph 2.

Article 9

Documentation and record keeping

1. High-risk AI systems shall be designed and developed so as to ensure that their outputs can be verified and traced back throughout the high-risk AI system's lifecycle, notably through the setting up of features allowing the automatic generation of logs.

2. The technical documentation shall contain all relevant information regarding the technical solutions used by the provider to ensure that high-risk AI systems comply with the requirements set out in Title III. It shall be drawn up before high-risk AI systems are placed on the market or put into service and shall be continuously updated.

3. The technical documentation shall be such as to demonstrate that the conformity of the high-risk AI system with the applicable requirements of this Regulation has been assessed and that the high-risk AI system complies with these requirements. It shall provide national competent authorities and notified bodies with all the information necessary to assess the compliance of the high-risk AI system with the requirements under this Regulation. At least, the technical documentation shall contain the elements set out in Annex IV.

4. Where a high-risk AI system referred to in Article 5(1) is placed on the market or put into service together with the product, the manufacturer of the product under the relevant Union harmonisation legislation shall draw-up a single technical documentation containing all the information as set out in Annex IV in addition to what is required under the relevant harmonisation legislation

5. The Commission is empowered to adopt delegated acts in accordance with Article 64 for the purpose of amending Annex IV in light of technical progress.

Article 10

Transparency and provision of information to users

1. High-risk AI systems shall be designed and developed so as to ensure that their operation is sufficiently transparent to enable users to understand and control how the high-risk AI system produces its output. The degree of transparency shall take into account the intended purpose of the high-risk AI systems and the need to ensure compliance with applicable legal obligations of the user and of the provider, as appropriate.

2. High-risk AI systems shall be accompanied by documentation and instructions of use in an appropriate digital format that are directed to users and include concise, clear and, to the extent possible, non-technical information that is relevant, accessible and understandable to the latter.

3. The information under paragraph 2 shall specify:

(a) the identity and the contact details of the provider and, where applicable, of their authorised representative;
(b) the high-risk AI systems' capabilities and limitations of performance, which shall at minimum include:
  (i) the intended purpose, [inclusive of the explicit indication of the specific context and the conditions under which the high-risk AI system can be expected to function as intended];
  (ii) the level of accuracy, robustness and security against which the high-risk AI system has been tested and validated and which can be expected;
  (iii) any known and foreseeable circumstances that may have an impact on the expected level of accuracy, robustness and security of the high-risk AI system;
  (iv) any known and foreseeable circumstances that may lead to unintended outcomes deriving from the use of the high-risk AI system and creating residual risks to safety and fundamental rights obligations, including known biases against specific groups protected under applicable EU non-discrimination law;
(c) the general logic, assumptions underlying the design choices including assumptions about persons or groups of persons relevant for determining the purpose and functionalities of the system; classification choices, and, for systems that make use of techniques involving the training of models with data, a description of the training data used for the development of the high-risk AI system, what the model is designed to optimise for and the weight accorded to the different parameters; *paragraph to verified and fine-tuned, in light also of Annex IV]*
(d) the technical and organisational human oversight measures referred to in Article 11, as well as any other mitigating or precautionary measures, which users shall take;
(e) the expected lifetime of the high-risk AI system and any necessary maintenance and care measures to ensure a proper functioning of the high-risk AI system, including as regards software updates.

Article 11

Human oversight

1. High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be overseen by natural persons through appropriate technical and/or organisational measures identified by the provider before the placing of the high-risk AI system on the market and to be implemented by the provider or the user as appropriate.

2. Human oversight shall serve the objective of preventing or minimising potential risks generated by a high-risk AI system, notably, but not exclusively, when such risks persist notwithstanding the application of other requirements established in this Regulation.

3. Organisational measures as referred to in paragraph 1 shall be identified so as to ensure that the natural persons to whom human oversight is assigned by the user have the competence, expertise training and authority necessary to carry out their role. As appropriate to the circumstances, the measures shall in particular be identified so as to ensure that the said natural persons:

(a) fully understand the capacities and limitations of the high-risk AI system and are able to duly monitor its operation so that signs of anomalies, dysfunctions and unexpected performance can be detected as soon as possible;
(b) have the expertise needed to operate the high-risk AI system and, upon detection of the signs under (a), can timely and meaningfully intervene to address them;
(c) do not automatically rely or over rely on the output generated by a high-risk AI system (automation bias), in particular for high-risk AI systems used to provide information or recommendations for decisions or determinations taken by natural persons;
(d) are able to correctly interpret the high-risk AI system's output, taking into account the characteristics of the high-risk AI system and the interpretation tools and methods available;
(e) can decide not to use the high-risk AI system or its outputs in any particular situation without any reason to fear negative consequences.

4. As appropriate to the circumstances, technical measures as referred to in paragraph 1 shall be identified so as to ensure that the high-risk AI system is subject to in-built operational constraints that cannot be overridden by the system itself and is responsive to the human intervention of the natural person to whom human oversight is assigned. In particular, the said natural person shall be able to:

(a) safely and instantly interrupt the operation of the high-risk AI system through a "stop" button or a similar procedure;
(b) disregard, correct, override or reverse the output of a high-risk AI system.

5. The lists in paragraphs 3 and 4 are not exhaustive and are without prejudice to any other organizational and technical measures that are suitable to achieve the objective stated in paragraph 2.

Article 12

Robustness, accuracy and security

1. High-risk AI systems shall perform consistently throughout their lifecycle in respect of their accuracy, robustness and security.

2. High-risk AI systems shall meet a high level of accuracy that is appropriate for their intended purpose and perform at the level of accuracy that is declared in the accompanying

documentation and instructions of use. High-risk AI systems shall indicate to the users the accuracy metric used and shall indicate when they do not meet the declared level of accuracy so that appropriate measures can be taken by the user.

3. High-risk AI systems shall meet a high level of robustness. They shall be resilient vis-à-vis errors, faults or inconsistencies that may occur within the system or in the environment in which the system operates, in particular due to their interaction with natural persons or other systems. The robustness of high-risk AI systems shall be achieved through technical redundancy solutions that are appropriate to the circumstances and the risks of the case; without prejudice to other options, technical solutions may include backup or fail-safe plans.

4. High-risk AI systems shall meet a high level of security. They shall be resilient vis-à-vis attempts to alter their use or performance by malicious third parties intending to exploit system vulnerabilities. The security of high-risk AI systems shall be achieved through technical solutions that are appropriate to the circumstances and the risks of the case; without prejudice to other options, technical solutions may include measures to prevent and control for data poisoning, adversarial examples or model flaws.

Chapter 2

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

Article 13

Obligations of providers of high-risk AI systems

1. Providers of high-risk AI systems shall ensure that these systems comply with the requirements listed in Chapter 1 of this Title.

2. Providers of high-risk AI systems shall put in place a quality management system that ensures compliance with this Regulation in the most effective and proportionate manner. The quality management system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions and shall address at least the following aspects:

(a) strategy for regulatory compliance, including compliance with conformity assessment procedures and procedures for the management of substantial modifications to the high-risk AI systems;
(b) techniques, procedures and systematic actions that will be used for the design, design control and design verification of high-risk AI systems;
(c) techniques, procedures and systematic actions that will be used for the development, quality control and quality assurance of high-risk AI systems;
(d) examinations, tests and validations procedures that will be carried out before, during and after the development of high-risk AI systems, and the frequency with which they will be carried out;

(e) technical specifications, including standards, that will be applied and, where the relevant harmonised standards will not be applied in full, the means that will be used to ensure that the high-risk AI systems comply with the requirements of this Regulation;
(f) systems and procedures for data management, including data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purposes of the placing on the market or putting into service of high-risk AI systems
(g) risk management system as set out in in Annex VIII;
(h) setting-up, implementation and maintenance of a post-market monitoring system, in accordance with Article 54;
(i) procedures related to the reporting of serious incidents and breaches of obligations under Union or Member States law intended to protect fundamental rights;
(j) handling of communication with national competent authorities, notified bodies, other economic operators, customers and/or other stakeholders;
(k) systems and procedures for record keeping of all relevant documentation and information;
(l) resource management, including selection and control of sub-contractors;
(m) accountability framework setting out the responsibilities of the management and other staff with regard to all aspects indicated above;

3. Providers of high-risk AI systems shall draw-up the technical documentation in accordance with Annex IV.

4. Providers of high-risk AI systems shall ensure that their systems undergo the relevant conformity assessment procedure in accordance with Article 35. Where compliance with the applicable requirements has been demonstrated following that conformity assessment, providers shall draw up an EU declaration of conformity in accordance with Article 38 and affix the CE marking of conformity in accordance with Article 39.

5. Providers shall keep records of the logs automatically generated by their high-risk AI systems.

6. A provider established outside the Union shall ensure that its authorised representative has the necessary documentation permanently available.

7. Providers shall comply with the registration obligations referred to in Articles 41.

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

9. Where the high-risk AI system presents a risk, providers shall immediately inform the national competent authorities of the Member States in which they made the system available

and, where applicable, the notified body that issued a certificate for the high-risk AI system, in particular of the non-compliance and of any corrective actions taken.

10. Providers shall, upon request by a national competent authority, provide it with all the information and documentation necessary to demonstrate the conformity of the high-risk AI system with the requirements of this Regulation, in an official Union language determined by the Member State concerned. Upon a reasoned request from a national competent authority, providers shall also give to that authority access to the logs automatically generated by the high-risk AI system.

11. Where a high-risk AI system referred to in Article 5(1) is placed on the market or put into service together with the product, the manufacturer of the product under the relevant legislation shall comply with the obligations of the provider established in this Regulation to the extent they are not covered already under the relevant Union harmonisation legislation, and notably ensure that the high-risk AI system complies with the requirements of this Regulation.

Article 14

Obligations of authorised representatives

1. A provider may, by a written mandate, appoint an authorised representative. An authorised representative shall always be appointed by a provider who is established outside the Union.

2. The obligations laid down in Article 13(1) to (4) shall not form part of the authorised representative's mandate.

3. An authorised representative shall perform the tasks specified in the mandate received from the provider. The mandate shall allow the authorised representative to do at least the following:

(a) keep a copy of the EU declaration of conformity and the technical documentation at the disposal of national competent authorities;
(b) upon a reasoned request from a national competent authority, provide that authority with all the information and documentation necessary to demonstrate the conformity of a high-risk AI system with the requirements of this Regulation;
(c) upon a reasoned request from a national competent authority, give to that authority access to the logs automatically generated by the high-risk AI system;
(d) cooperate with the competent national authorities on any action taken by the latter, at their request.

Article 15

Obligations of importers

1. Importers shall place on the Union market only high-risk AI systems that comply with the requirements of this Regulation.

2. Before placing a high-risk AI system on the market, importers shall ensure that the appropriate conformity assessment procedure has been carried out by the provider. They shall

ensure that the provider has drawn up the technical documentation and that the high-risk AI system bears the required conformity marking and is accompanied by the required documentation and instructions if use.

3. Where an importer considers or has reason to believe that a high-risk AI system is not in conformity with this Regulation, they shall not place the high-risk AI system on the market until it has been brought into conformity. Furthermore, where the high-risk AI system presents a risk, the importer shall inform the provider and the market surveillance authorities to that effect.

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

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

6. Upon a reasoned request from a national competent authority, importers shall provide it with all the information and documentation necessary to demonstrate the conformity of a high-risk AI system with the requirements set out in this Regulation in a language which can be easily understood by that authority. They shall also cooperate with the competent national authorities on any action taken by the latter.

Article 16

Obligations of distributors

1. When making a high-risk AI system available on the market, distributors shall act with due care in relation to the obligations applicable to them.

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

3. Where a distributor considers or has reason to believe that a high-risk AI system is not in conformity with this Regulation, they shall not make the high-risk AI system available on the market until it has been brought into conformity. Furthermore, where the system presents a risk, the distributor shall inform to that effect the provider or the importer, as applicable.

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

5. Distributors who consider or have reason to believe that a high-risk AI system which they have made available on the market is not in conformity with this Regulation shall make sure that the corrective actions necessary to bring that system into conformity, to withdraw it or

recall it, if appropriate, are taken. Furthermore, where the high-risk AI system presents a risk, distributors shall immediately inform the competent national authorities of the Member States in which they made the product available to that effect, giving details, in particular, of the non-compliance and of any corrective actions taken.

6. Upon a reasoned request from a national competent authority, distributors shall provide it with all the information and documentation necessary to demonstrate the conformity of a high-risk system with the requirements set out in this Regulation. They shall also cooperate with that authority on any action taken by the latter.

Article 17

Cases in which obligations of providers apply to distributors, importers or any other third-party

Any distributor, importer or other third-party, including the user, shall be considered a provider for the purposes of this Regulation and shall be subject to the obligations of the provider under Article 13, where they place on the market or put into service a high-risk AI system under their name or trademark or modify the intended purpose of a high-risk AI system already placed on the market or put into service, or makes a substantial modification to the high-risk AI system.

Article 18

Obligations of users of high-risk AI systems

1. Users of high-risk AI systems shall use such systems in accordance with the instructions of use and take all technical and organisational measures indicated by the providers to address residual risks posed by the use of high-risk AI systems, taking into account the intended purpose of the high-risk AI system.

2. Without prejudice to any other existing legal obligation addressed to them, users may take additional technical and organisational measures considered appropriate, provided that they are not incompatible with those indicated by the providers.

3. Users shall monitor the operation of the high-risk AI systems for evident anomalies or irregularities, [including as regards the automatic generation of logs if relevant information has been communicated to him by the provider]. For high-risk AI systems that continue to 'learn' after being placed on the market or put into service, they shall in particular monitor, on the basis of the documentation and instructions of use, the occurrence of any changes to the high-risk AI system and its performance.

3. Users of high-risk AI systems shall keep records of the description of the input data used for the operation of the high-risk AI systems that continue to 'learn' after being placed on the market or put into service [when such input data is not in accordance with the instructions of use of the high-risk AI system].

4. Users of high-risk AI systems shall use the information provided under Article 12 to comply with their obligation to carry out a data protection impact assessment under Article 35 of

Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680 of the European Parliament and of the Council[32], where applicable.

Article 19

Obligations of third parties involved in the artificial intelligence value chain

1. Without prejudice to the providers' obligations and responsibilities, third parties shall ensure that the terms and conditions of sale and supply, also without remuneration, of software, software tools and components, pre-trained models, data and other services in relation to the high-risk AI systems do not prevent providers, importers, distributors or users from meeting any of their obligations under this Regulation.

2. Third parties shall cooperate with providers, importers, distributors, authorised representatives and users of high-risk AI systems to ensure compliance with this Regulation within their capacities and responsibilities.

Chapter 3

NOTIFIED BODIES

Article 20

Competence of notified bodies under this Regulation

1. For high-risk AI systems referred to in Article 5(1), notified bodies which have been notified under that relevant Union harmonisation legislation shall be entitled to control the conformity of the high-risk AI systems with the requirements in Title III [as applicable], provided that their compliance with requirements under Article 22(4), (9), (10) has been assessed in the context of the notification procedure under the relevant Union harmonisation legislation.

2. For other high-risk AI systems, notified bodies which have been designated and notified in accordance with this Regulation shall be entitled to conduct the relevant conformity assessment in accordance with Article 35.

Article 21

National competent authorities responsible for notified bodies designated under this Regulation

1. Any Member State that intends to designate a conformity assessment body as a notified body under this Regulation shall appoint a national competent authority that shall be responsible for

[32] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89–131).

setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring.

2. The national competent authority responsible for notified bodies shall be established and organised so as to safeguard the objectivity and impartiality of its activities.

3. The national competent authority responsible for notified bodies shall have a sufficient number of competent personnel permanently available for the proper performance of its tasks. Competences shall include an in-depth understanding of artificial intelligence technologies, data and data computing, knowledge of fundamental rights and existing standards and legal requirements.

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

Article 22

Requirements related to notified bodies designated under this Regulation

1. Notified bodies shall fulfil the tasks for which they are designated in accordance with this Regulation.

2. They shall satisfy the organisational and general requirements and the quality management, resource and process requirements that are necessary to fulfil those tasks.

3. The organisational structure, allocation of responsibilities, reporting lines and operation of the notified body shall be such that they ensure that there is confidence in the performance by the notified body and in the results of the conformity assessment activities it conducts.

4. The notified body shall be a third-party body that is independent of the provider of high-risk AI systems in relation to which it performs conformity assessment activities. The notified body shall also be independent of any other economic operator or public body having an interest in the artificial intelligence field as well as of any competitors of the provider.

5. The notified body shall be organised and operated so as to safeguard the independence, objectivity and impartiality of its activities. The notified body shall document and implement a structure and procedures for safeguarding impartiality and for promoting and applying the principles of impartiality throughout its organisation, personnel and assessment activities.

6. The notified body shall have documented procedures in place ensuring that its personnel, committees, subsidiaries, subcontractors and any associated body or personnel of external bodies respect the confidentiality of the information which comes into its possession during the performance of conformity assessment activities, except when disclosure is required by law.

7. The notified body shall take out appropriate liability insurance for its conformity assessment activities, unless liability is assumed by the Member State in question in accordance with national law or that Member State is directly responsible for the conformity assessment.

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

9. The notified body shall have sufficient internal competence to critically evaluate assessments conducted by external expertise. Such requirement presupposes at all times and for each conformity assessment procedure and each type of high-risk AI system in relation to which they have been designated, that the notified body has permanent availability of sufficient administrative, technical and scientific personnel who possess experience and knowledge relating to the relevant artificial intelligence technologies, data and data computing and to the requirements of this Regulation.

10. The staff of the notified body shall be bound to observe professional secrecy with regard to all information obtained in carrying out its tasks under this Regulation, except vis-à-vis the national competent authorities of the Member State in which its activities are carried out.

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

12. Notified bodies shall make available and submit upon request all relevant documentation, including the provider's documentation, to the national competent authority referred to in Article 22 to allow it to conduct its assessment, designation, notification, monitoring and surveillance activities and to facilitate the assessment outlined in this Chapter.

Article 23

Subsidiaries of and subcontracting by notified bodies

1. Where a notified body subcontracts specific tasks connected with the conformity assessment or has recourse to a subsidiary, it shall ensure that the subcontractor or the subsidiary meets the requirements set out in Article 22 and shall inform the notifying authority accordingly.

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

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

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

Article 24

Application of notified bodies designated under this Regulation

1. A conformity assessment body shall submit an application for notification to the national competent authority of the Member State referred to in Article 22 in which it is established.

2. The application for notification shall be accompanied by a description of the conformity assessment activities, the conformity assessment module or modules and the artificial intelligence technologies for which that body claims to be competent, as well as by an accreditation certificate, where one exists, issued by a national accreditation body attesting that the conformity assessment body fulfils the requirements laid down in Article 22. Any valid document related to existing designations of the applicant notified body under any other Union harmonisation legislation shall be inserted.

3. Where the conformity assessment body concerned cannot provide an accreditation certificate, it shall provide the notifying authority with all the documentary evidence necessary for the verification, recognition and regular monitoring of its compliance with the requirements laid down in Article 19. For notified bodies which are designated under any other Union harmonisation legislation, all documents and certificates linked to those designations can be used to support their designation procedure under this Regulation, to the extent appropriate.

Article 25

Notification procedure

1. National competent authorities referred to in Article 7 may notify only conformity assessment bodies which have satisfied the requirements laid down in Article 22.

2. They shall notify the Commission and the other Member States using the electronic notification tool developed and managed by the Commission.

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

4. The [conformity assessment] body concerned may perform the activities of a notified body only where no objections are raised by the Commission or the other Member States within one month of a notification.

5. The national competent authority referred to in Article 23 shall notify the Commission and the other Member States of any subsequent relevant changes to the notification.

Article 26

Identification numbers and lists of notified bodies designated under this Regulation

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

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

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

Article 27

Changes to notifications

1. Where a national competent authority referred to in Article 21 has ascertained or has been informed that a notified body no longer meets the requirements laid down in Article 22, or that it is failing to fulfil its obligations, that authority shall restrict, suspend or withdraw the notification as appropriate, depending on the seriousness of the failure to meet those requirements or fulfil those obligations. It shall immediately inform the Commission and the other Member States accordingly.

2. In the event of restriction, suspension or withdrawal of notification, or where the notified body has ceased its activity, the national competent authority shall take appropriate steps to ensure that the files of that notified body are either processed by another notified body or kept available for the responsible competent authorities at their request.

Article 28

Challenge of the competence of notified bodies

1. The Commission shall investigate all cases where it doubts, or doubt is brought to its attention, regarding the competence of a notified body or the continued fulfilment by a notified body of the requirements and responsibilities to which it is subject.

2. The Member State shall provide the Commission, on request, with all information relating to the basis for the notification or the maintenance of the competence of the notified body concerned.

3. The Commission shall ensure that all sensitive information obtained in the course of its investigations is treated confidentially.

4. Where the Commission ascertains that a notified body does not meet or no longer meets the requirements for its notification, it shall adopt an implementing act requesting the notifying Member State to take the necessary corrective measures, including withdrawal of notification if necessary. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 65(2).

Article 29

Appeal against decisions of notified bodies

Member States shall ensure that an appeal procedure against decisions of the notified bodies is available.

Article 30

Information obligations of notified bodies

1. Notified bodies shall inform the national competent authority referred to in Article 22 of the following:

(a) any refusal, restriction, suspension or withdrawal of an EU technical documentation assessment certificate or a quality management system approval in accordance with the requirements of Annex VI;
(b) any circumstances affecting the scope of or conditions for notification;
(c) any request for information which they have received from market surveillance national competent authorities regarding conformity assessment activities;
(d) on request, conformity assessment activities performed within the scope of their notification and any other activity performed, including cross-border activities and subcontracting.

2. Notified bodies shall provide the other bodies notified under this Regulation carrying out similar conformity assessment activities covering the same artificial intelligence technologies with relevant information on issues relating to negative and, on request, positive conformity assessment results.

Article 31

Exchange of experience

The Commission shall provide for the organisation of exchange of experience between the national competent authorities responsible for notification policy.

Article 32

Coordination of notified bodies

1. The Commission shall ensure that appropriate coordination and cooperation between bodies notified under this Regulation are put in place and properly operated in the form of a sectoral group of notified bodies**.**

2. Member States shall ensure that the bodies notified by them participate in the work of that group, directly or by means of designated representatives.

3. Relevant issues related to high-risk AI systems referred to in Article 5(1) shall be discussed by the coordination groups of notified bodies established under those Union harmonisation legislations. However, those groups shall coordinate and exchange as appropriate with the coordination group of notified bodies established under this Regulation to ensure a consistent approach of notified bodies activities in the field of artificial intelligence.

Chapter 4

CONFORMITY ASSESSMENT, STANDARDS, CERTIFICATES, REGISTRATION

Article 33

Harmonised standards

1. High-risk AI systems which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements set out in Title III, as applicable, covered by those standards or parts thereof.

2. Paragraph 1 shall also apply to system or process requirements to be fulfilled in accordance with this Regulation by providers of high-risk AI systems, including those relating to quality management, risk management and post-market monitoring systems.

3. By way of derogation to this Article, Article 8 of Directive 2014/90/EU of the European Parliament and of the Council[33] shall apply for high-risk AI systems covered under that Directive.

Article 34

Common specifications

1. Where no harmonised standards exist or where relevant harmonised standards are not sufficient, or where there is a need to address specific safety or fundamental right concerns, the Commission may, by means of implementing acts, adopt common specifications in respect of the requirements set out in Title III, including the technical documentation, and post-market monitoring. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 65(2).

2. When common specifications specifically concern a high-risk AI system referred to in Article 5(1), the involvement of any relevant expert sectorial groups or body established under the relevant Union harmonisation legislation shall be ensured.

3. High-risk AI systems which are in conformity with the common specifications referred to in paragraph 1 shall be presumed to be in conformity with the requirements of this Regulation covered by those common specifications or the relevant parts of those common specifications.

4. Providers shall comply with the common specifications referred to in paragraph 1, unless they can duly justify that they have adopted technical solutions that ensure a level of safety and performance that is at least equivalent thereto.

[33] Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC (Text with EEA relevance) (OJ L 257, 28.8.2014, p. 146–185).

Article 35

Conformity assessment

1. The provider shall perform a conformity assessment of the high-risk AI system with a view to demonstrating its conformity with the requirements set out in Title III as applicable.

2. High-risk AI systems which have been trained and tested solely on data generated in the Union shall be presumed to be in compliance with the requirement set out in Article 8(5).

3. For high-risk AI systems referred to in Article 5(1), providers shall follow the relevant conformity assessment as foreseen under the relevant Union harmonisation legislation. However the requirements set out in Title III as applicable are applicable to the high-risk AI system and shall be part of that conformity assessment. Points 4.3, 4.4., 4.5 and subparagraph 4 of point 4.6 and subparagraph 3 of point 4.8 of Annex VI remain also applicable.

4. For high-risk AI systems referred to in Annex II, paragraph 3, after drawing up the technical documentation referred to in Article 42, providers shall carry out a conformity assessment by themselves. Where they have assessed that their high-risk AI system is in compliance with the requirements of this Regulation, they shall declare the conformity of their high-risk AI system by issuing the EU declaration of conformity referred to in Article 38.

5. For high-risk AI systems referred to in Annex II, paragraph 2, where, in assessing the compliance of a high-risk AI system with the requirements set out in Title III as applicable, the provider has applied harmonised standards the references of which have been published in the Official Journal of the European Union, they may opt to carry out a conformity assessment by themselves. Where they have assessed that the high-risk AI system is in compliance with the requirements of this Regulation, the provider shall declare the conformity of the high-risk AI system by issuing the EU declaration of conformity referred to in Article 38 after drawing up the technical documentation referred to in Annex IV. Where, in assessing the compliance of a high-risk AI system with the requirements set in Title III as applicable, the provider has not applied or has applied only in part harmonised standards the references of which have been published in the Official Journal of the European Union, or where such harmonised standards do not exist, they shall follow the conformity assessment with the applicable conformity assessment procedure set out in Annex VI.

6. For all high-risk AI systems, a provider shall undergo a new conformity assessment of the high-risk AI system whenever they operate a substantial modification of the high-risk AI system, regardless of whether the modified high-risk AI system is intended to be further distributed or continues to be used by the current user. For high-risk AI systems that continue to 'learn' after being placed on the market or put into service, changes to the high-risk AI system and its performance which have not been pre-determined at the moment of the initial conformity assessment and are not part of the information contained in the technical documentation under point d) of Annex IV shall be considered substantial modifications. When a substantial modification is operated by a third-party, other than the provider, that party shall assume all

obligations incumbent on the provider, including undergoing a new conformity assessment of the high-risk AI system in question.

7. The Commission is empowered to adopt delegated acts in accordance with Article 64 for the purpose of updating Annex VI in light of technical progress.

Article 36

Certificates

1. The certificate issued by the notified bodies in accordance with Annex VI shall be in an official Union language determined by the Member State in which the notified body is established or otherwise in an official Union language acceptable to the notified body.

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

3. Where a notified body finds that the requirements of this Regulation are no longer met by the provider, it shall, taking account of the principle of proportionality, suspend or withdraw the certificate issued or impose any restrictions on it, unless compliance with such requirements is ensured by appropriate corrective action taken by the provider within an appropriate deadline set by the notified body. The notified body shall give the reasons for its decision.

Article 37

Derogation from conformity assessment procedure

1. By way of derogation from Article 35, any market surveillance authority may authorise, for exceptional reasons of public security or protection of life and health of natural persons and the protection of industrial and commercial property, the placing on the market or putting into service within the territory of the Member State concerned of specific high-risk AI systems even though the applicable conformity assessment procedures, including the affixing of CE marking, have not been completed in accordance with this Regulation. Such authorisation shall be for a limited period of time, while the necessary conformity assessment procedures are being carried out and at the latest until those procedures have been completed.

2. The authorisation mentioned in paragraph 1 shall be issued only if the market surveillance authority concludes that the high-risk AI system complies in substance with the requirements of this Regulation. The market surveillance authority shall inform the Commission and the other Member States of any authorisation issued pursuant to paragraph 1.

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

4. Where, within 15 days of receipt of the notification referred to in paragraph 2, objections are raised by a Member State against an authorisation issued by a market surveillance authority of another Member State, or where the Commission considers the authorisation to be contrary to Union law, the Commission shall without delay enter into consultation with the relevant Member State and economic operator or operators and evaluate the authorisation. On the basis of the results of that evaluation, the Commission shall decide whether the authorisation is justified or not. The Commission shall address its decision to the Member State concerned and shall immediately communicate it to it and the relevant economic operator or operators.

5. If the authorisation is considered unjustified, this shall be withdrawn by the market surveillance authority of the Member State concerned.

6. For high-risk AI systems intended to be used as safety components of devices, or which are themselves devices, covered by Regulation (EU) 2017/745 and Regulation (EU) 2017/746, Article 59 of Regulation (EU) 2017/745 and Article 54 of Regulation (EU) 2017/746 shall also apply with regard to the derogation from the conformity assessment of the compliance with the requirements of this Regulation.

Article 38

EU declaration of conformity

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

2. Where high-risk AI systems are subject to other Union harmonisation legislation which also requires an EU declaration of conformity, a single EU declaration of conformity shall be drawn up in respect of all Union legislations applicable to the high-risk AI system. The declaration shall contain all the information required for identification of the Union harmonisation legislation to which the declaration relates.

3. By drawing up the EU declaration of conformity, the provider shall assume responsibility for compliance with the requirements of this Regulation. The provider shall continuously update the EU declaration of conformity as appropriate.

4. The Commission shall is empowered to adopt delegated acts in accordance with Article 64 for the purpose of updating the content of the EU declaration of conformity set out in Annex V in light of technical progress.

Article 39

CE marking of conformity

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

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

3. Where applicable, the CE marking shall be followed by the identification number of the notified body responsible for the conformity assessment procedures set out in Article 42. The identification number shall also be indicated in any promotional material which mentions that the high-risk AI system fulfils the requirements for CE marking.

4. By way of derogation from this Article, Article 9 of Directive 2014/90/EU on marine equipment shall apply for high-risk AI systems covered under that Directive.

Article 40

Registration

1. Before placing a high-risk AI systems on the market or putting it into service, the provider or, where applicable the authorised representative, shall register that high-risk AI system in the database referred to in Article 52. To this purpose, it shall enter the information referred to in Annex VII and shall thereafter keep the information updated.

2. For high-risk AI systems covered by any of the legislations referred to in Article 5(1), and where those legislations foresee registration systems at the EU level, the provider shall not be required to fulfil the obligation set in paragraph 1 of this Article.

TITLE IV

TRANSPARENCY OBLIGATIONS FOR CERTAIN OTHER AI SYSTEMS

Article 41

Transparency obligations for certain other AI systems

Without prejudice to the requirements and obligations for high-risk AI systems under Title III,

1. providers of AI systems shall ensure that AI systems intended to interact with natural persons are designed and developed in such a manner that natural persons are notified that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use,

2. any natural person whose personal data is being processed by an emotion recognition system or a categorisation system shall be notified that they are exposed to such a system,

3. users of AI systems who use the same to generate or manipulate image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a reasonable person to be authentic [or truthful], shall disclose that the content has been artificially created or manipulated. This obligation shall not apply where necessary for the purposes of safeguarding public security [and other prevailing public interests] or for the

exercise of a legitimate right or freedom of a person and subject to appropriate safeguards for the rights and freedoms of third parties.

TITLE V

OBLIGATIONS FOR THE USE OF REMOTE BIOMETRIC IDENTIFICATION SYSTEMS

Article 42

Remote biometric identification systems in publicly accessible places

1. Without prejudice to the requirements and obligations laid down in Title III, Member States and Union institutions and bodies shall ensure that an authorisation system is put in place for the use of remote biometric identification systems in publicly accessible spaces.

2. The use of remote biometric identification systems in publicly accessible places shall be allowed only:

(a) [optional] where authorised by Union or Member State law;
(b) [optional] to serve the objective of preventing, detecting or investigating serious crime and terrorism[34],
(c) [optional] limited to a temporal scope [optional: of [6] hours per day] and a geographical scope [optional: of 30% of a given local entity]. Users may derogate from these limitations in exceptional circumstances in a state of emergency declared by the competent authorities.
(d) with a valid EU declaration of conformity for the remote biometric identification system's intended purpose and the technical documentation as set out in Article 38;

3. The authorising decision shall be based on:

(a) A data protection impact assessment fulfilling the requirements as laid down in:
    (i) Article 35(7) of Regulation (EU) 2016/679;
    (ii) or Article 27(2) of Directive (EU) 2016/680;
    (iii) or Article 39(7) of the Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data[35];

[34] As defined in 2002/584/JHA: Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States – and DIRECTIVE 2014/41/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 3 April 2014 regarding the European Investigation Order in criminal matters

[35] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and

(b) The Impact Assessment shall include:
   (i) Evidence of the accuracy for the use of the system for the given purpose, including an assessment of potential impacts on different groups in the population;
   (ii) An assessment of safeguards put in place to ensure that there is sufficient protection for different groups in the population, in particular for vulnerable groups;
   (iii) Considerations on the system's consistency with Union values and considerations on the impact on democracy at large.

Article 43

Procedural requirements for the authorisation of the use of remote biometric identification systems in publicly accessible spaces

1. Authorising authority shall be the supervisory authority

(a) as referred to in Chapter VI of Regulation (EU) 2016/679,
(b) or as referred to in Chapter VI of Directive (EU) 2016/680,
(c) or as referred to in Chapter VI of Regulation (EU) 2018/1725.

2. Before giving or refusing authorisation, the authorising authority shall publish a summary of the planned use of the remote biometric identification system in publicly accessible spaces for at least 15 working days for public comments. A notice thereof shall be published in the public database of registered high-risk AI systems. [The authorising authority shall consider the input received.]

3. At least 15 working days before giving or refusing authorisation, the supervisory authority shall inform the European Data Protection Board and the European Artificial Intelligence Board of its draft decision.

4. The European Data Protection Board and the European Artificial Intelligence Board shall ensure consistency of decisions under paragraph 3 and for that purpose adopt recommendations. [OR can object the draft decision within 10 working days.]

5. An authorisation decision may be subject to obligations and conditions for the use of the remote biometric identification system in publicly accessible places, including mandating specific changes to the system, additional testing requirements and renotification requirements.

6. The validity of the decision can be limited in time or expire in case substantial modifications are made affecting the functioning of the system.

7. The authorising authority shall publish the final decision. A notice thereof shall be published in the public database of registered high-risk AI systems.

agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.) (OJ L 295, 21.11.2018, p. 39–98).

TITLE VI

MEASURES IN SUPPORT OF INNOVATION

Article 44

AI regulatory sandboxing schemes

1. AI regulatory sandboxing schemes may be established by national competent authorities from one or more Member States and/or the European Data protection Supervisor to facilitate the development and testing of innovative AI systems under strict regulatory oversight before AI systems are placed on the market or otherwise put into service. Member States shall ensure that, to the extent the innovative AI systems involve the processing of personal data or otherwise fall under the supervisory remit of other national competent authorities, the national data protection authorities and these other national competent authorities shall be associated to the artificial intelligence regulatory sandboxing scheme.

2. The objectives of the artificial intelligence regulatory sandboxing schemes shall be to:

(a) foster artificial intelligence innovation by establishing a controlled experimentation and testing environment which enables constructive cooperation between competent authorities and innovators and facilitates supervised development, testing and validation of AI systems, while integrating appropriate protections and safeguards in compliance with relevant Union and Member States legislation;
(b) enhance competent authorities' oversight and understanding of the opportunities, emerging risks and the impacts of artificial intelligence innovation on the economy, the society and fundamental rights and provide them with a flexible and agile regulatory tool to learn from experience, closely monitor developments and draw lessons and identify any amendments needed to the legal framework applicable to AI systems;
(c) [Minimize the costs and the legal risks of non-compliance for participants experimenting with artificial intelligence technology and accelerate access to markets, including by removing barriers for SMEs and start-ups to enter the market and scale up.]

3. The artificial intelligence regulatory sandboxing schemes shall facilitate the cooperation between the competent authorities designated under Article 50 and other competent authorities responsible for supervising compliance of the innovative AI system with the applicable sectoral Union and Member States legislation.

4. Where appropriate, an infrastructural environment for testing and experimentation for the artificial intelligence regulatory sandboxing schemes shall be provided by the Testing Experimentation Facilities referred to in Article 46 or by other appropriate labs and testing facilities established within the Member States or at cross-border level through joint initiatives.

5. Participation in the artificial intelligence regulatory sandboxing schemes shall not affect the supervisory and corrective powers of the competent authorities and shall allow them to exercise their discretionary powers and levers of proportionality granted by applicable Union and

Member States legislation when interpreting and implementing the legal requirements to concrete AI systems participating in the sandboxing scheme.

6. Participants in the sandboxing schemes shall remain liable under applicable Union and Member States liability legislation for any harm inflicted on third parties as a result from the experimentation taking place in the artificial intelligence regulatory sandboxing scheme(s).

7. Without prejudice to obligations pursuant to applicable Union legislation, Member States establishing artificial intelligence regulatory sandboxing schemes shall coordinate their activities and cooperate within the framework of the European Artificial Intelligence Board under Article 47 to ensure a common European approach to artificial intelligence innovation.

8. The modalities of the operation of the artificial intelligence sandboxing schemes, including the eligibility criteria and the procedure for the application, selection, participation and exiting from the artificial intelligence regulatory sandboxing schemes and the obligations and the rights of the participants shall be defined through implementing acts in accordance with the examination procedure referred to in Article 65(2).

Article 45

Measures to reduce the regulatory burden for SMEs/start-ups

1. To reduce the regulatory burden on the Small and Medium Enterprises (SMEs) and start-ups for compliance with this Regulation, the national competent authorities shall undertake the following actions:

(a) provide SMEs and start-ups with priority access to the artificial intelligence regulatory sandboxes to the extent that they fulfil the eligibility conditions specified in Article 41(7) and have made proposals that are of similar value compared to proposals of larger companies;
(b) organize specific awareness raising activities about the application of this Regulation tailored to the needs of the SMEs and start-ups;
(c) establish a dedicated channel [hub] within the national competent authorities' organisational structure for informal communication with SMEs and other innovators to provide guidance and respond to queries about the implementation of this Regulation.

2. Notified bodies shall take into account the specific interests and needs of the SMEs and start-ups when setting the fees for conformity assessment under Article 35 and reduce them proportionately.

3. SMEs shall be provided with priority access and privileged conditions for the use of the services provided by the Digital Hubs and Testing Experimentation Facilities under Article 46 of this Regulation.

Article 46

Digital Hubs and Testing Experimentation Facilities

1. Digital Hubs and Testing Experimentation Facilities as established in accordance with [Digital Europe Program legal act], shall contribute to the implementation of this Regulation, by offering their expertise and services to providers and notified bodies when carrying out their respective obligations foreseen by this Regulation.

2. For the purpose of the implementation of the Regulation, Digital Hubs and Testing Experimentation Facilities may have the following tasks as appropriate:

(a) provide relevant training to providers on the requirements of this Regulation;
(b) upon request, provide relevant technical and scientific support as well as testing facilities to providers, in order to support them in ensuring that their AI systems comply with the requirements of this Regulation;
(c) upon request, provide technical and scientific opinions to Notified Bodies, as well as testing facilities, in order to support those Bodies in the context of a conformity assessment procedure carried out in accordance with Article 35.

3. The Commission may adopt implementing acts to determine the operational aspects related to the tasks to be carried out by digital hubs and testing in the context of this Regulation.

4. The Commission may require providers and notified bodies to pay fees for the services provided by Digital Hubs and Testing Experimentation Facilities. The structure and the level of fees as well as the scale and structure of recoverable costs shall be adopted by the Commission by means of implementing acts, taking into account the objectives of the adequate implementation of this Regulation, support of innovation and SMEs. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 65(2).

TITLE VII

GOVERNANCE

Article 47

European Artificial Intelligence Board

1. A European Artificial Intelligence Board (the 'Board') shall be established. The Board shall be composed of one representative per each national supervisory authority, [the European Data Protection Supervisor] and a representative of the European Commission. Each national supervisory authority shall designate to the Board a representative who is competent to perform the tasks set out below. The Board shall adopt its own rules of procedure by a simple majority of its members. The rules of procedure shall also contain the operational aspects related to the Board's tasks as listed in Article 48.

2. The activities of the Board will be supported by a Secretariat provided by the European Commission and by an expert group referred to in Article 49 that shall be set up by the Commission.

Article 48

Tasks of the European Artificial Intelligence Board

1. The Board shall carry out the following tasks as laid out below:

(a) it shall supervise the consistent application of this Regulation by the Member States, including by issuing opinions or interpretative guidance documents; [whenever the Board intends to issue opinions or interpretative guidance documents with regard to AI systems in areas covered under other Union legislation, the Board shall consult any relevant body or relevant expert group which is established under that Union legislation, as appropriate];
(b) it shall collect and share best practices among Member States;
(c) it shall contribute and participate in the development of artificial intelligence-related harmonised standards or common specifications, as specified in Articles 33 and 34;
(d) it shall provide advice and expertise to the Commission and other Union institutions, agencies and bodies on specific questions related to artificial intelligence, including for the purposes of paragraph 2 below;
(e) it shall continuously monitor technical and market developments related to artificial intelligence, including their impact on the health and safety and the fundamental rights and freedoms of persons;
(f) it shall ensure consistency and coordination in the functioning of the artificial intelligence regulatory sandboxes referred to in Article 44;

2. Before the Commission adopts a delegated act pursuant to Article 64, the Board shall issue an opinion to the Commission. The Board shall request the expert group referred to in Article 49 to identify, gather, and assess any relevant information and elements necessary to determine whether other AI systems generate a high level of risk of harm in the same way as the high-risk AI systems in Annex II. Whenever those other AI systems relate to areas covered under other Union legislation, the Board shall consult any relevant body or relevant expert group which is established under that Union legislation.

3. In carrying out its activities, the Board shall exchange with stakeholders on a regular basis and ensure that their opinions and views can inform its activities to an appropriate extent.

4. The Board shall carry out its tasks in close cooperation with other relevant bodies and structures established at EU level, including the European Data Protection Board, the EU network of market surveillance, [the Consumer Protection Cooperation (CPC) network] as well as other sectoral bodies and authorities at EU level. Such cooperation shall be without prejudice to the independence and the powers granted by Union law to the Board and any other authority or body established at EU level.

Article 49

Provision of technical and scientific advice to the Board

1. The Commission shall appoint by way of an implementing act an expert group to provide technical and scientific advice to the Board referred to in Article 47. The implementing act shall specify, inter alia, the details related to the composition of the group, its operation and the remuneration of experts.

2. The expert group shall consist of independent experts appointed for a renewable three-year term by the Commission on the basis of their scientific or technical expertise in the field and taking into account the tasks of the Board as referred in Article 48.

3. The Commission shall appoint a number of experts which is deemed to be sufficient to fulfil the foreseen needs, taking into particular account the need to ensure a smooth application of Article 48(2). In addition to the permanent experts, in consultation with the Board and when a specific expertise is required, the Commission can appoint additional experts for a limited period of time.

4. The Commission shall establish systems and procedures to manage and prevent potential conflicts of interest. Declarations of interests shall be made publicly available.

5. The appointed experts shall perform their tasks with the highest level of professionalism, independence, impartiality and objectivity.

6. The experts shall be remunerated for their preparatory work and participation (in person or by electronic means) in the meetings of the expert group and in other requested activities. Travel and, where appropriate, subsistence expenses of experts shall be reimbursed by the Commission in accordance with the provisions in force at the Commission.

7. When adopting positions, views and reports, the expert group shall attempt to reach consensus. If consensus cannot be reached, decisions shall be taken by simple majority of the group members.

Article 50

Designation of competent authorities responsible for the implementation of the Regulation

1. Without prejudice to the competences of the judicial and administrative authorities under existing Union and Member States legislation, each Member State shall designate one or more national competent authorities and, among them, the national supervisory authority, for the purpose of supervising the application and implementation of this Regulation, or parts thereof.

2. Member States shall inform the Commission, the Board and the other competent authorities of other Member States accordingly. At their own initiative, Member States may also establish one central contact point for communication with the providers and users, provided that effective coordination is ensured between all responsible competent authorities.

3. Member States shall ensure that all national competent authorities are provided with sufficient financial and human resources, expertise and competencies in the fields of artificial

intelligence, fundamental rights and safety risks to effectively achieve the aims of and fulfil their tasks under this Regulation.

4. National competent authorities shall provide guidance and advice on the implementation of this Regulation, including to SMEs and start-ups. Whenever national competent authorities intend to provide guidance and advice with regard to an AI system in areas covered under other Union legislation, the national authorities which are competent under that Union legislation shall be consulted, as appropriate.

5. The European Data Protection Supervisor shall act as a competent authority for the supervision of the EU institutions, agencies and bodies when falling within the scope of this Regulation. It shall be provided with the necessary financial and human resources, expertise and competencies in the fields of artificial intelligence, fundamental rights and safety risks to effectively achieve the aims of and fulfil its tasks under this Regulation.

Article 51

Obligation of cooperation

1. All operators listed in Title III shall cooperate with the national competent authorities regarding actions initiated and requested by the latter, including investigations.

2. The operators shall cooperate with the national competent authorities, at the request of the latter and in specific cases, to facilitate any action to eliminate or, if that is not possible, to mitigate the risks presented by an AI system that has been placed on the Union market.

TITLE VIII

EU DATABASE FOR HIGH-RISK AI SYSTEMS

Article 52

EU database on high-risk AI systems

1. The Commission shall, in collaboration with the Member States, set up and maintain an EU database at Union level.

2. The EU database shall contain the data regarding high-risk AI systems which are registered in accordance with Article 40.

3. The data shall be entered into the EU database by the providers. The Commission shall provide them with technical and administrative support.

4. All the information collated and processed in the EU Database shall be accessible to the public.

5. The EU database shall contain personal data only insofar as necessary for the electronic systems referred to in paragraph 2 of this Article to collate and process information in

accordance with this Regulation. That information shall include the names and contact details of natural persons who are responsible for registering the system and have the legal authority to represent the provider.

6. The Commission and the Member States shall ensure that data subjects may effectively exercise their rights to information, of access, to rectification and to object in accordance with Regulation (EU) 2018/1725 and Regulation (EU) 2016/679, respectively. They shall also ensure that data subjects may effectively exercise the right of access to data relating to them, and the right to have inaccurate or incomplete data corrected and erased. Within their respective responsibilities, the Commission and the Member States shall ensure that inaccurate and unlawfully processed data are deleted, in accordance with the applicable legislation.

7. In relation to its responsibilities under this Article and the processing of personal data involved therein, the Commission shall be considered to be the controller of the database and its electronic systems.

Article 53

Functionality of the database

1. The Commission shall, in collaboration with the Board referred to in Article 47, draw up the functional specifications for the EU database referred to in Article 52. The Commission shall draw up a plan for the implementation of those specifications by (1 year after entry into force). That plan shall seek to ensure that the database is fully functional at a date that allows the Commission to publish the notice referred to in paragraph 3 of this Article by (2 months before application of Regulation).

2. The Commission shall, on the basis of an independent audit report, inform the Board when it has verified that the database has achieved full functionality and meets the functional specifications drawn up pursuant to paragraph 1.

3. The Commission shall, after consultation with the Board and when it is satisfied that the conditions referred to in paragraph 2 have been fulfilled, publish a notice to that effect in the Official Journal of the European Union.

TITLE IX

POST-MARKET MONITORING, INFORMATION SHARING, MARKET SURVEILLANCE

Section I

Post-market monitoring

Article 54

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

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

2. The post-market monitoring system shall be intended to actively and systematically collect, document and analyse relevant data provided by users or collected through other sources on the performance of high-risk AI systems throughout their lifetime, and to evaluate the continuous compliance of AI systems with the requirements of this Regulation.

3. The post-market monitoring system shall be based on a post-market monitoring plan. The post-market monitoring plan shall be part of the technical documentation specified in Annex IV.

4. For AI systems covered by any of the legislations referred to in Annex III, where a post-market monitoring system and plan is already established under that legislation, the aspects described under paragraphs 1 to 3 of this Article shall be integrated into that system and plan as appropriate.

5. If, in the course of the post-market monitoring operations, a need for preventive or corrective actions or both is identified by the provider, the provider shall implement the appropriate measures and inform, where applicable, the notified body and users.

Section II

Sharing of information on artificial intelligence incidents and malfunctioning

Article 55

Reporting of incidents and breaches of obligations under applicable legislation intended to protect fundamental rights

1. Providers of high-risk AI systems placed on the Union market shall report to the relevant national competent authorities any serious incidents or any malfunctioning of the AI system

which constitutes a breach of obligations under Union and Member States law intended to protect fundamental rights.

2. Providers shall report any serious breaches of obligations referred to in paragraph 1 above no later than 15 days after they become aware of that breach.

3. Providers shall report any serious incident, immediately after they have established the causal relationship between that incident and the AI system or that such causal relationship is reasonably possible and not later than 15 days after they become aware of the incident.

4. In order to facilitate compliance of providers with the obligations set out in paragraphs 2 and 3 of this Article, the Board referred to in Article 47 shall develop dedicated guidance. This guidance shall be issued 1 year before the entry into application of this Regulation at the latest.

5. The obligations set under the previous paragraphs of this Article shall be without prejudice to any other reporting obligations set under other Union law.

6. For high-risk AI systems covered by Regulation (EU) 2017/745 and Regulation (EU) 2017/746, the applicability of this Article shall be limited to reporting of breaches of obligations under Union and Member States law intended to protect fundamental rights.

Section III

Enforcement

Article 56

Market surveillance and control of AI systems in the Union market

1. Regulation (EU) 2019/1020 shall apply to the AI systems covered by this Regulation. However, for the purpose of the effective enforcement of this Regulation:

(a) any reference to economic operator under Regulation (EU) 2019/1020 shall be intended as including all operators identified in Chapter 2 of Title III of this Regulation;
(b) any reference to product under Regulation (EU) 2019/1020 shall be intended as including all AI systems under the scope of this Regulation.

2. National supervisory authorities shall report to the Board on a regular basis the outcomes of relevant market surveillance activities in order to support the Board in fulfilling its tasks, including with regard to the amendment of the list of high-risk AI systems as referred to in Article 5(3).

3. For AI systems covered by any of the Union harmonisation legislations referred to in Annex III, the market surveillance authority for the purposes of this Regulation shall be the authority responsible for market surveillance activities designated under the relevant Union harmonisation legislation. The provisions of this Section shall apply insofar as they are not covered under the relevant Union harmonisation legislation.

4. With regard to AI systems referred to in Annex II, paragraph 3, Member States should consider entrusting market surveillance activities for those systems to the national competent authorities already designated under relevant sectoral Union legislation, where applicable.

5. Without prejudice to the powers and competences of Member States in organising their market surveillance activities regarding AI systems, Member States shall facilitate the coordination between market surveillance authorities designated under this Regulation and other relevant national authorities or bodies which supervise the application of other relevant Union and Member States legislation that might be concerned by the use [or development] of a particular AI system in their territory.

6. Where relevant, market surveillance authorities, may carry out joint investigations with the authorities of other Member States in cross border cases.

7. When planning their activities, market surveillance authorities shall give appropriate consideration to AI systems which have not been or only partially trained and tested on datasets generated in the Union, notably with regard to their conformity with the requirement set out in Article 8(5).

Article 57

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

1. AI systems presenting a risk shall be understood as referring to Article 3(19) of Regulation (EU) 2019/1020.

2. Where the market surveillance authority of a Member State has sufficient reason to believe that an AI system covered by this Regulation presents a risk to the health or safety of persons or to the protection of fundamental rights, they shall carry out an evaluation of the AI system concerned in respect of its compliance with all the requirements laid down in this Regulation. The relevant economic operators shall cooperate as necessary with the market surveillance authorities.

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

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

3. Where the market surveillance authority referred to in paragraph 2 considers that non-compliance is not restricted to its national territory, it shall inform the Commission and the

other Member States of the results of the evaluation and of the actions which it has required the economic operator to take.

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

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

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

6. The information referred to in paragraph 5 shall include all available details, in particular the data necessary for the identification of the non-compliant AI system, the origin of the AI system, the nature of the non-compliance alleged and the risk involved, the nature and duration of the national measures taken and the arguments put forward by the relevant economic operator. In particular, the market surveillance authorities shall indicate whether the non-compliance is due to either:

(a) failure of the AI system to meet requirements relating to the health or safety of persons or to the protection of fundamental rights or to other aspects of public interest protection laid down in this Regulation; or
(b) shortcomings in the harmonised standards or common specifications referred to in conferring a presumption of conformity.

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

8. Where, within three months of receipt of the information referred to in paragraph 5, no objection has been raised by either a Member State or the Commission in respect of a provisional measure taken by a Member State, that measure shall be deemed justified.

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

Article 58

Union safeguard procedure

1. Where, within three months of receipt of the notification referred to in Article 57, objections are raised by a Member State against a measure taken by another Member State, or where the Commission considers the measure to be contrary to Union law, the Commission shall without

delay enter into consultation with the relevant Member State and economic operator or operators and shall evaluate the national measure. On the basis of the results of that evaluation, the Commission shall decide whether the national measure is justified or not.

The Commission shall address its decision to all Member States and shall immediately communicate it to them and the relevant economic operator or operators.

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

3. Where the national measure is considered justified and the non-compliance of the AI system is attributed to shortcomings in the harmonised standards or common specifications referred to in Articles 33 and 34, the Commission shall apply the procedure provided for in Article 11 of Regulation (EU) No 1025/2012.

Article 59

Compliant AI systems which present a risk

1. Where, having performed an evaluation under Article 56, a Member State finds that although an AI system is in compliance with this Regulation, it presents a risk to the health or safety of persons, to the compliance with obligations under Union or member States legislation intended to protect fundamental rights or to other aspects of public interest protection, it shall require the relevant economic operator to take all appropriate measures to ensure that the AI system concerned, when placed on the market or put into service, no longer presents that risk, to withdraw the AI system from the market or to recall it within a reasonable period, commensurate with the nature of the risk, as it may prescribe.

2. The provider or other responsible operators shall ensure that corrective action is taken in respect of all the AI systems concerned that they have made available on the market throughout the Union.

3. The Member State shall immediately inform the Commission and the other Member States. That information shall include all available details, in particular the data necessary for the identification of the AI system concerned, the origin and the supply chain of the system, the nature of the risk involved and the nature and duration of the national measures taken.

4. The Commission shall without delay enter into consultation with the Member States and the relevant operator and shall evaluate the national measures taken. On the basis of the results of that evaluation, the Commission shall decide whether the measure is justified or not and, where necessary, propose appropriate measures.

5. The Commission shall address its decision to all Member States and shall immediately communicate it to them and the relevant economic operator or operators.

Article 60

Formal non-compliance

1. Without prejudice to Article 56, where a Member State makes one of the following findings, it shall require the relevant provider to put an end to the non-compliance concerned:

(a) the conformity marking has been affixed in violation of Article 39;
(b) the conformity marking has not been affixed;
(c) the EU declaration of conformity has not been drawn up;
(d) the EU declaration of conformity has not been drawn up correctly;
(e) the identification number of the notified body, where the conformity assessment procedure is applied, has not been affixed;
(f) the technical documentation is either not available or not complete.

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

TITLE X

CODES OF CONDUCT

Article 61

Codes of conduct

1. The Commission and the Board shall encourage and facilitate the drawing up of codes of conduct intended to foster the voluntary application of the requirements established in Title IV of this Regulation to AI systems other than high-risk AI systems pursuant to Article 5. Codes of conduct shall include the technical specifications that will be adhered to in order to ensure compliance of the AI systems covered by the codes of conduct with the said requirements.

2. Codes of conduct may further contain a voluntary commitment to meet additional requirements, provided that the codes of conduct set out clear objectives and contain key performance indicators to measure the achievement of those objectives. Such additional requirements may relate to environmental sustainability, accessibility to persons with disability, stakeholders participation in the design and development of the AI systems, diversity of the development teams.

3. Codes of conduct may be drawn up by individual providers of AI systems and/or by organisations representing them. Providers and their representative organisations may involve users and their representative organisations as well as any interested stakeholder or representative organisation of stakeholders.

4. Codes of conduct may cover one or more AI systems. When including more than one AI system in a code of conduct, the provider shall demonstrate that the application of a single code

of conduct is appropriate taking into account the similarity of the intended purpose of the AI systems.

TITLE XI

CONFIDENTIALITY AND PENALTIES

Article 62

Confidentiality

1. Without prejudice to existing national provisions and practices in the Member States on confidentiality, all parties involved in the application of this Regulation shall respect the confidentiality of information and data obtained in carrying out their tasks in order to protect the following:

(a) personal data, in accordance with Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EU) 2018/1725;
(b) commercially confidential information and trade secrets of a natural or legal person, including intellectual property rights; unless disclosure is in the public interest;
(c) the effective implementation of this Regulation, in particular for the purpose of inspections, investigations or audits.

2. Without prejudice to paragraph 1, information exchanged on a confidential basis between the national competent authorities and between national competent authorities and the Commission shall not be disclosed without the prior agreement of the originating national competent authority.

3. Paragraphs 1 and 2 shall not affect the rights and obligations of the Commission, Member States and notified bodies with regard to the exchange of information and the dissemination of warnings, nor the obligations of the persons concerned to provide information under criminal law.

4. The Commission and Member States may exchange confidential information with regulatory authorities of third countries with which they have concluded bilateral or multilateral confidentiality arrangements.

Article 63

Penalties

1. Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate, and dissuasive. [The Member States

shall notify the Commission of those rules and of those measures by XXX and shall notify it, without delay, of any subsequent amendment affecting them.]

2. The following infringements shall, in accordance with paragraph 3, be subject to administrative fines up to [20 000 000] EUR, or in the case of an undertaking, up to [4] % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the development, placing on the market or putting into service of an AI system enlisted under Article 4 (Prohibited AI practices);
(b) the supply of incorrect, incomplete or false information to notified bodies;
(c) non-compliance with the obligation to cooperate with the national competent authorities pursuant to Article 51 (Obligation for cooperation).

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

(a) the nature, gravity and duration of the infringement and of its consequences;
(b) the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement.

4. Each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

TITLE XII

DELEGATED ACTS & COMITOLOGY

Article 64

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The delegation of power referred to in Articles 3(2), 6(1), 6(8), 9(5), 35(6) and 38(4) shall be conferred on the Commission for an indeterminate period of time from entering into force of the Regulation.

3. The delegation of power referred to in Articles 3(2), 6(1), 6(8), 9(5), 35(6) and 38(4) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Articles 3(2), 6(1), 6(8), 9(5), 35(6) and 38(4) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Article 65

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

TITLE XIII

FINAL PROVISIONS

Article 66

Relationship with other Union legislation

This Regulation is without prejudice to the provisions of existing Union legislation applicable to artificial intelligence falling within the scope of this Regulation.

Article 67

Transitional provisions for high-risk AI systems that are already covered by an EU certificate or have already been placed on the market or put into service

High-risk AI systems referred to in Article 5(1) which are covered by a valid EU certificate issued before the date of application of this Regulation as set in Article 69 and high-risk AI systems listed in Annex II, paragraph 2 which have been placed on the Union market or put into service before the date of application of this Regulation as set in Article 69 shall be brought into compliance with this Regulation within [XX months] from the date of application of this Regulation as set in Article 69.

Article 68

Evaluation and review

1. The Commission shall assess the need for amendment of the list in Annexe III every 6 months [once per year] following the entry into force of this Regulation.

2. Three years after this Regulation becomes applicable and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.

3. Three years after the present Regulation becomes applicable and every four years thereafter, the Commission shall evaluate the impact and effectiveness of codes of conduct to foster the application of the requirements established in Title IV of this Regulation and possibly other additional requirements to AI systems other than high-risk AI systems.

3. For the purpose of paragraphs 1, 2 and 3, the Commission may request information from the Board, the Member States and competent authorities.

4. In carrying out the evaluations and reviews referred to in paragraphs 1, 2 and 3, the Commission shall take into account the positions and findings of the expert group referred to in Article 49, of the European Parliament, of the Council, and of other relevant bodies or sources.

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

Article 69

Entry into force

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

2. It shall apply from ….. [or one or two year following the entering into force of the Regulation or more].

3. Chapter 3 of Title III (Notified Bodies) shall apply as from three months following the entry into force of this Regulation.

4. Title VII (Governance) shall apply as from six months following the entry into force of this Regulation.

ANNEX I

ARTIFICIAL INTELLIGENCE TECHNIQUES AND APPROACHES

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

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

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

ANNEX II

HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEMS

1. AI systems listed in this Annex shall be classified as high-risk AI systems.

2. High-risk AI systems listed in this paragraph are subject to third party conformity assessment pursuant to Article 35(4):

(a) AI systems intended to be used for the remote biometric identification of persons in publicly accessible spaces;

(b) AI systems intended to be used as safety components in the management and operation of essential public infrastructure networks, such as [roads or] the supply of water, gas and electricity.

3. High-risk AI systems listed in this paragraph are subject to self-assessment of conformity pursuant to Article 35(3):

(a) AI systems intended to be used to dispatch or establish priority in the dispatching of emergency first response services, including by firefighters and medical aid;
(b) AI systems intended to be used for the purpose of determining access or assigning persons to educational and vocational training institutions, as well as for assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions;
(c) AI systems intended to be used for recruitment – for instance in advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests – as well as for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating work performance and behaviour;
(d) AI systems intended to be used to evaluate the creditworthiness of persons;
(e) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility for public assistance benefits and services, as well as to grant, revoke, or reclaim such benefits and services;
(f) AI systems intended to be used for making individual risk assessments, or other predictions intended to be used as evidence, or determining the trustworthiness of information provided by a person with a view to prevent, investigate, detect or prosecute a criminal offence or adopt measures impacting on the personal freedom of an individual;
(g) AI systems intended to be used for predicting the occurrence of crimes or events of social unrest with a view to allocate resources devoted to the patrolling and surveillance of the territory;

(h) AI systems intended to be used for the processing and examination of asylum and visa applications and associated complaints and for determining the eligibility of individuals to enter into the territory of the EU;
(i) AI systems intended to be used to assist judges at court, except for ancillary tasks.

ANNEX III

LIST OF UNION HARMONISATION LEGISLATION

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

2. Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (OJ L 170, 30.6.2009, p. 1);

3. Directive 2014/33/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to lifts and safety components for lifts (OJ L 96, 29.3.2014, p. 251);

4. Directive 2014/34/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to equipment and protective systems intended for use in potentially explosive atmospheres (OJ L 96, 29.3.2014, p. 309);

5. Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014, p. 62);

6. Directive 2014/68/EU of the European Parliament and of the Council of 15 May 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of pressure equipment (OJ L 189, 27.6.2014, p. 164);

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

8. Regulation (EU) 2016/424 of the European Parliament and of the Council of 9 March 2016 on cableway installations and repealing Directive 2000/9/EC (OJ L 81, 31.3.2016, p. 1);

9. Regulation (EU) 2016/426 of the European Parliament and of the Council of 9 March 2016 on appliances burning gaseous fuels and repealing Directive 2009/142/EC (OJ L 81, 31.3.2016, p. 99);

10. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1);

11. Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).

ANNEX IV

TECHNICAL DOCUMENTATION

[content and language to be further verified and fine-tuned]

The technical documentation shall, wherever applicable, contain at least the following elements:

(a) a general description of the AI system including:
  (i) its intended purpose;
  (ii) how the system interacts or can be used to interact with hardware or software that is not part of the system itself, where applicable;
  (iii) the versions of relevant software or firmware and any requirement related to version update;
  (iv) the description of all forms in which the AI system is placed on the market or put into service;
  (v) the description of hardware on which the AI system is intended to run;
  (vi) where the AI system is a component of products, photographs or illustrations showing external features, marking and internal layout of those products;
  (vii) instructions of use for the user and installation instructions, where applicable;
(b) a description of the main elements of the AI system and of the process for its development, including:
  (i) description of the methods and steps performed for the development of the AI system, including, where relevant, the recourse to pre-trained systems or tools provided by third parties and how these have been modified and used by the provider;
  (ii) information about the conceptual design and the algorithms, including the rationale and assumptions underlying the design choices, including assumptions about persons or groups of persons relevant for determining the purpose and functionalities of the system; main classification choices made; what the model is designed to optimise for and the weight accorded to the different parameters, decisions about any trade-off between conflicting principles/requirements;
  (iii) the programming code(s), the description of system architecture explaining how software components build on or feed into each other and integrate into the overall processing, the computational resources used to build, test and validate the AI systems;
  (iv) where relevant, datasheets describing the training methodologies, techniques and training data sets used, including information about the provenance of the training data, its scope and main characteristics, how the data was obtained and selected, labelling procedures (for supervised learning only), the outliers (detecting points in a database that are unusual in supervised learning);
  (v) assessment of the technical and organisational human oversight measures needed in accordance with Article 13;

(vi) where applicable, a detailed description of pre-determined algorithm changes and changes in performance of the AI systems, together with all the relevant information related to technical solutions envisaged to ensure continuous compliance of the system with the relevant requirements;

(vii) detailed information about testing and validation procedures used, including information about the testing data used and their main characteristics, metrics used to measure accuracy, fairness and potentially discriminatory impacts, security and other relevant requirements; [test logs and all test reports dated and signed by the responsible person(s); this information shall be provided also with regard to pre-determined algorithm and performance changes as referred to under point (f).]

(viii) [input problem definition, the expected output and the control parameters].

(c) detailed information about the functioning of the validated AI system, describing its capabilities and limitations, anticipated inputs and outputs, expected accuracy/error margin, , including limitations in the performance and known biases against specific groups protected under applicable Union non-discrimination law, the foreseeable unintended consequences and sources of risks to safety and fundamental rights in view of the context of application, the affected persons and any foreseeable misuse, the required human oversight procedures and any user information and installation instructions [where applicable];

(d) risk management procedures under Annex VIII;

(e) a list of the harmonised standards applied in full or in part the references of which have been published in the Official Journal of the European Union, and, where those harmonised standards have not been applied, descriptions of the solutions adopted to meet the requirements set out in Title III, as applicable, including a list of other relevant technical specifications applied. In the event of partly applied harmonised standards, the technical documentation shall specify the parts which have been applied;

(f) copy of the EU declaration of conformity;

(g) a description of the system in place to evaluate the AI system performance in the post-market phase in accordance with Article 54.

ANNEX V

EU DECLARATION OF CONFORMITY

The EU declaration of conformity shall contain all of the following information:

1. AI system name and type and any additional unambiguous reference allowing identification and traceability of the AI system;

2. Name and address of the provider or, where applicable, their authorised representative;

3. A statement that the EU declaration of conformity is issued under the sole responsibility of the provider;

4. A statement that the AI system in question is in conformity with this Regulation and, if applicable, with any other relevant Union legislation that provides for the issuing of an EU declaration of conformity;

5. References to any relevant harmonised standards used or any other common specification in relation to which conformity is declared;

6. Where applicable, the name and identification number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued;

7. Where applicable, additional information;

8. Place and date of issue of the declaration, name and function of the person who signed it as well as an indication for, and on behalf of whom, that person signed, signature.

ANNEX VI

CONFORMITY BASED ON ASSESSMENT OF QUALITY MANAGEMENT SYSTEM AND ASSESSMENT OF TECHNICAL DOCUMENTATION

1. Conformity based on quality management system plus assessment of the technical documentation is the conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2 to 6, and ensures and declares on their sole responsibility that the AI system concerned satisfies the requirements of this Regulation that apply to it.

2. Development

The provider shall operate an approved quality management system for the design, development and testing of the AI system in accordance with Article 13(2) and shall be subject to surveillance as specified in point 5. The technical documentation of the AI system shall be examined in accordance with point 4.

3. Quality management system

3.1. The provider shall lodge an application for assessment of their quality management system with the notified body of their choice, for the AI system concerned.

The application shall include:

(a) the name and address of the provider and, if the application is lodged by the authorised representative, their name and address as well;
(b) the list of AI systems covered under the same quality management system
(b) the technical documentation for each AI system covered under the same quality management system;
(c) the documentation concerning the quality management system which shall cover all the aspects listed under Article 13(2);
(d) a description of the procedures in place to ensure that the quality management system remains adequate and effective;
(e) a written declaration that the same application has not been lodged with any other notified body.

3.2. The notified body shall assess the quality management system to determine whether it satisfies the requirements referred to in Article 13(2).

The provider or their authorised representative shall be notified of the decision.

The notification shall contain the conclusions of the quality management system assessment and the reasoned assessment decision.

3.3. The provider shall undertake to fulfil to implement the quality management system as approved and to maintain it so that it remains adequate and efficient.

3.4. The provider shall inform the notified body that has approved the quality management system of any intended change to the quality management system or the list of AI systems covered by the latter.

The notified body shall evaluate any proposed changes and decide whether the modified quality management system will continue to satisfy the requirements referred to in point 3.2 or whether a reassessment is necessary.

It shall notify the provider of its decision. The notification shall contain the conclusions of the examination and the reasoned assessment decision.

3.5 Each notified body shall inform its notifying authorities of quality management system approvals issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of quality system approvals refused, suspended or otherwise restricted.

Each notified body shall inform the other notified bodies of quality management system approvals which it has refused, suspended or withdrawn, and, upon request, of quality system approvals which it has issued.

4. Control of the technical documentation

4.1. In addition to the application referred to in point 3, the provider shall lodge an application for the assessment of the technical documentation relating to the AI system which it intends to place on the market or put into service and which is covered by the quality management system referred to under point 3.

4.2. The application shall include:

— the name and address of the provider;

— a written declaration that the same application has not been lodged with any other notified body;

— the technical documentation as referred to in Annex IV.

4.3. The notified body shall examine the application. In this context, the notified body shall be granted full access to the training and testing datasets used by the provider, including through application programming interfaces (API) or other appropriate means and tools enabling remote access.

4.4. In examining the application, the notified body shall give appropriate consideration to AI systems which have not been or only partially trained and tested on datasets generated in the Union, notably with regard to their conformity with the requirement set out in Article 8(5).

4.5 In examining the application, the notified body may require that the provider supplies further evidence or carries out further tests so as to enable a proper assessment of conformity of the AI system with the requirements of this Regulation. Whenever the notified body is not

satisfied with the tests carried out by the provider, the notified body shall directly carry out adequate tests, as appropriate.

4.6 Where the AI system is in conformity with the requirements of this Regulation, the notified body shall issue an EU technical documentation assessment certificate. The certificate shall indicate the name and address of the provider, the conclusions of the examination, the conditions (if any) for its validity and the data necessary for the identification of the AI system.

The certificate and its annexes shall contain all relevant information to allow the conformity of the AI system to be evaluated, and to allow for control of the AI system while in use , where applicable.

Where the AI system is not in conformity with the requirements of this Regulation, the notified body shall refuse to issue an EU technical documentation assessment certificate and shall inform the applicant accordingly, giving detailed reasons for its refusal.

Where the AI system does not meet the requirement relating to the data used to train it, re-training of the AI system will be needed prior to the application for a new conformity assessment. In this case, the reasoned assessment decision of the notified body refusing to issue the EU technical documentation assessment certificate shall contain specific considerations on the quality data used to train the AI system and recommendations to achieve compliance therewith.

4.7 Any change to the AI system that could affect the operation of AI system or its intended purpose shall be approved by the notified body which issued the EU technical documentation assessment certificate. The provider shall inform such notified body of its intention to introduce any of the above-mentioned changes. The notified body shall assess the intended changes and decide whether they require a new conformity assessment in accordance with Article 35(5) or whether they could be addressed by means of a supplement to the EU technical documentation assessment certificate. In the latter case, the notified body shall assess the changes, notify the provider of its decision and, where the changes are approved, issue to the provider a supplement to the EU technical documentation assessment certificate.

4.8. Each notified body shall inform its notifying authorities of the EU technical documentation assessment certificates and/or any supplements thereto which it has issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of certificates and/or any supplements thereto refused, suspended or otherwise restricted.

Each notified body shall inform the other notified bodies of the EU technical documentation assessment certificates and/or any supplements thereto which it has refused, withdrawn, suspended or otherwise restricted, and, upon request, of the certificates and/or supplements thereto which it has issued.

The notified body shall also inform the notifying authority of the EU technical documentation assessment certificates which it has refused, withdrawn, suspended or otherwise restricted due to lack of compliance with Article 15.

On request, the Commission, the national competent authorities and the other notified bodies may obtain a copy of the EU technical documentation assessment certificate and/or supplements thereto. On request, the Commission and the national competent authorities may obtain a copy of the technical documentation and of the results of the examinations carried out by the notified body.

The notified body shall keep a copy of the EU technical documentation assessment certificate, its annexes and supplements, as well as of the application including the documentation and all other evidence and materials submitted by the provider until the expiry of the validity of the certificate.

5. Surveillance under the responsibility of the notified body

5.1. The purpose of the surveillance carried out by the notified body is to make sure that the provider duly fulfils the terms and conditions of the approved quality management system.

5.2. For assessment purposes, the provider shall allow the notified body to access the premises where the design, development, testing of the AI systems is taking place. Upon request of the notified body, the provider shall allow access to relevant data, documentation or information through application programming interfaces (API) or other appropriate means and tools enabling remote access. The provider shall further share with the notified body all necessary information, in particular:

(a) the quality management system documentation;
(b) the quality records as provided for by the design part of the quality system, such as results of analyses, calculations, tests, etc.;
(c) the quality records as provided for by the development part of the quality management system, such as inspection reports and test data, reports concerning the qualifications of the personnel, etc.

5.3. The notified body shall carry out periodic audits to make sure that the provider maintains and applies the quality management system and shall provide the provider with an audit report. In the context of those audits, the notified body may carry out additional tests of the AI systems for which an EU technical documentation assessment certificate was issued.

6. CE marking and EU declaration of conformity

6.1. The provider shall affix the CE marking in accordance with Article 39 and, under the responsibility of the notified body referred to in point 3.1, the latter's identification number to each AI system that satisfies the applicable requirements set out in Title III as applicable.

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

A copy of the EU declaration of conformity shall be given to the relevant national competent authorities upon request.

6.3 The provider shall, for a period ending 10 years after the AI system has been placed on the market or put into service, keep at the disposal of the national competent authorities: (a) the technical documentation referred to in point 3.1; (b) the documentation concerning the quality management system referred to in point 3.1; (c) the documentation concerning the changes referred to in point 3.5, as approved; (d) the decisions and other documents issued of the notified body referred to in points 4.5 and 4.6.

ANNEX VII

INFORMATION TO BE SUBMITTED UPON THE REGISTRATION OF HIGH-RISK AI SYSTEMS IN ACCORDANCE WITH ARTICLE 40

The following information shall be provided and thereafter kept up to date with regard to high-risk AI systems to be registered in accordance with Article 40.

1.1. Type of economic operator (provider, authorised representative);

1.2. Name, address and contact details of the economic operator;

1.3. Where submission of information is carried out by another person on behalf of any of the economic operators mentioned under Section 1.1, the name, address and contact details of that person;

1.4 AI system trade name and any additional unambiguous reference allowing identification and traceability of the AI system;

1.5. Description of the intended purpose of the AI system;

1.6. Status of the AI system (on the market, no longer placed on the market, recalled);

1.7. Type, number and expiry date of the certificate issued by the notified body and the name or identification number of that notified body;

1.8. A scanned copy of the certificate referred to in Section 1.7;

1.9. Member States in which the AI system is to or has been placed on the market, put into service or made available in the Union;

1.10. A copy of the EU declaration of conformity referred to in Article 38;

1.11. Electronic instructions for use;

1.12 URL for additional information (optional).

ANNEX VIII

RISK MANAGEMENT SYSTEM

1. Providers of high-risk AI systems shall establish, implement, document and maintain a risk management system.

2. Risk management shall be understood as a continuous iterative process throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating. In carrying out risk management providers shall:

(a) identify and analyse the known and foreseeable hazards associated with each high-risk AI system;
(b) estimate and evaluate the risks associated with, and occurring during, the use of the high-risk AI system according to its intended purpose and under conditions of reasonably foreseeable misuse;
(c) eliminate or mitigate the risks referred to in point (b) through risk management measures, in accordance with the provisions of paragraphs 3 to 7;
(d) evaluate and estimate possibly arising risks based on the analysis of data gathered from the post-market surveillance system.

3. Risk management measures shall give due consideration to the effects and possible interactions resulting from the combined application of the requirements established in Title III. Risk management measures shall take into account the generally acknowledged state of the art, including as reflected in relevant harmonised standards or common specifications.

4. Providers shall manage risks so that the residual risk associated with each hazard as well as the overall residual risk is judged acceptable. In identifying the most appropriate risk management measures, providers shall:

(a) eliminate or reduce risks as far as possible through safe design and development;
(b) where appropriate, take adequate mitigation and control measures in relation to risks that cannot be eliminated; and
(c) provide relevant information (such as warnings/precautions) and, where appropriate, training to users.

5. Providers shall thoroughly test high-risk AI systems for the purposes of identifying the most appropriate risk management measures. Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and they are in compliance with the requirements and obligations established in this Regulation and other Union or Member States law on safety and fundamental rights.

6. Testing procedures shall be proportionate to the intended purpose of the AI system and do not need to go beyond what is necessary to achieve their objective.

7. The testing of the high-risk AI systems shall be performed, as appropriate, at any point in time throughout the development process, and, under all circumstances, prior to the placing on the market or the putting into service. [Testing shall be made against preliminarily defined metrics and probabilistic thresholds that are appropriate to the intended purpose of the high-risk AI system].

8. Testing procedures and results as well as any appropriate mitigating and correcting measures taken as a consequence of the testing shall be documented.

9. Providers of AI systems shall inform users of any residual risks. In eliminating or reducing risks related to error pu, the provider shall give due consideration to the technical knowledge, experience, education, training and use environment.