European Parliament

Committee on the Internal Market and Consumer Protection
Committee on Civil Liberties, Justice and Home Affairs

9/5/2023

KMB/DA/AS

Version: 1.0

DRAFT Compromise Amendments

on the Draft Report

Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts

(COM(2021)0206 – C9 0146/2021 – 2021/0106(COD))

Rapporteurs:
Brando Benifei & Ioan-Dragoş Tudorache

(Joint committee procedure – Rule 58 of the Rules of Procedure)

Title III, Chapter 4 and recitals 65 and 65a	CA 1

(65) In order to carry out third-party conformity assessments ***when so required***, 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, absence of conflicts of ***interests and minimum cybersecurity requirements***. ***Member States should encourage the designation of a sufficient number of conformity assessment bodies, in order to make the certification feasible in a timely manner. The procedures of assessment, designation, notification and monitoring of conformity assessment bodies should be implemented as uniformly as possible in Member States, with a view to removing administrative border barriers and ensuring that the potential of the internal market is realised.***

(65a) In line with Union commitments under the World Trade Organization (WTO) Agreement on Technical Barriers to Trade (TBT), it is adequate to maximise the acceptance of test results produced by competent conformity assessment bodies, independent of the territory in which they are established, where necessary to demonstrate conformity with the applicable requirements of the Regulation. The Commission should actively explore possible international instruments for that purpose and in particular pursue the possible establishment of mutual recognition agreements with countries which are on a comparable level of technical development, and have compatible approach concerning AI and conformity assessment.

CHAPTER 4

NOTIFIYING AUTHORITIES AND NOTIFIED BODIES

Article 30
Notifying authorities

1. Each Member State shall designate or establish a notifying authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring. ***These procedures shall be developed in cooperation between the notifying authorities of all Member States.***
2. Member States may designate a national accreditation body referred to in Regulation (EC) No 765/2008 as a notifying authority.
3. Notifying authorities shall be established, organised and operated in such a way that no conflict of interest arises with conformity assessment bodies and the objectivity and impartiality of their activities are safeguarded.
4. Notifying authorities shall be organised in such a way that decisions relating to the notification of conformity assessment bodies are taken by competent persons different from those who carried out the assessment of those bodies.
5. Notifying authorities shall not offer or provide any activities that conformity assessment bodies perform or any consultancy services on a commercial or competitive basis.

6. Notifying authorities shall safeguard the confidentiality of the information they obtain.

7. Notifying authorities shall have a sufficient number of competent personnel at their disposal for the proper performance of their tasks. ***Where applicable, competent personnel shall have the necessary expertise, such as a degree in an appropriate legal field, in supervision of fundamental rights enshrined in the Charter of Fundamental rights of the Union.***

8. Notifying authorities shall make sure that conformity assessments are carried out in a proportionate ***and timely*** manner, avoiding unnecessary burdens for providers**,** and that notified bodies perform their activities taking due account of the size of an undertaking, the sector in which it operates, its structure and the degree of complexity of the AI system in question. ***Particular attention shall be paid to minimising administrative burdens and compliance costs for micro and small enterprises as defined in Commission Recommendation 2003/361/EC.***

Article 31
Application of a conformity assessment body for notification

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

2. The application for notification shall be accompanied by a description of the conformity assessment activities, the conformity assessment module or modules and the artificial intelligence technologies for which the conformity assessment body claims to be competent, as well as by an accreditation certificate, where one exists, issued by a national accreditation body attesting that the conformity assessment body fulfils the requirements laid down in Article 33. Any valid document related to existing designations of the applicant notified body under any other Union harmonisation legislation shall be added.

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

Article 32
Notification procedure

1. Notifying authorities ***shall*** notify only conformity assessment bodies which have satisfied the requirements laid down in Article 33.

2. Notifying authorities shall notify the Commission and the other Member States using the electronic notification tool developed and managed by the Commission ***of each conformity assessment body referred to in paragraph 1***.

3. The notification ***referred to in paragraph 2*** shall include full details of the conformity assessment activities, the conformity assessment module or modules and the artificial intelligence technologies concerned***, as well as the relevant attestation of competence.***

4. The conformity assessment body concerned may perform the activities of a notified body only where no objections are raised by the Commission or the other Member States within ***two weeks of the validation of the*** notification ***where it includes an accreditation certificate referred to in Article 31(2), or within two months of the notification where it incudes documentary evidence referred to in Article 31(3).***

4a. Where objections are raised, the Commission shall without delay enter into consultation with the relevant Member States and the conformity assessment body. In view thereof, the Commission shall decide whether the authorisation is justified or not. The Commission shall address its decision to the Member State concerned and the relevant conformity assessment body.

4b. Member States shall notify the Commission and the other Member States of conformity assessment bodies.

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

Article 33
Notified bodies

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

2. Notified bodies shall satisfy the organisational, quality management, resources and process requirements that are necessary to fulfil their tasks ***as well as the minimum cybersecurity requirements set out for public administration entities identified as operators of essential services pursuant to Directive XXX on measures for a high common level of cybersecurity across the Union (NIS2), repealing Directive (EU) 2016/1148.***

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

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

4a. Conformity assessment pursuant to paragraph 1 shall be performed by employes of notified bodies who have not provided any other other service related to the matter assessed than the conformity assessment to the provider of a high-risk AI system nor to any legal person connected to that provider in the 12 months' period before the assessment and have committed to not providing them with such services in the 12 months' period after the completion of the assessment.

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

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

6. Notified bodies shall have documented procedures in place ensuring that their personnel, committees, subsidiaries, subcontractors and any associated body or personnel of external bodies respect the confidentiality of the information which comes into their possession during the performance of conformity assessment activities, except when disclosure is required by law. The staff of notified bodies shall be bound to observe professional secrecy with regard to all information obtained in carrying out their tasks under this Regulation, except in relation to the notifying authorities of the Member State in which their activities are carried out. ***Any information and documentation obtained by notified bodies pursuant to the provisions of this Article shall be treated in compliance with the confidentiality obligations set out in Article 70.***

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

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

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

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

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

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

Article 34
Subsidiaries of and subcontracting by notified bodies

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

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

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

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

Article 35
Identification numbers and lists of notified bodies ~~designated under this Regulation~~

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

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

Article 36
Changes to notifications

1. Where a notifying authority has suspicions or has been informed that a notified body no longer meets the requirements laid down in Article 33, or that it is failing to fulfil its obligations, that authority shall without delay investigate the matter with the utmost diligence. In that context, it shall inform the notified body concerned about the objections raised and give it the possibility to make its views known. If the notifying authority comes to the conclusion that the notified body ~~investigation~~ no longer meets the requirements laid down in Article 33 or that it is failing to fulfil its obligations, it shall restrict, suspend or withdraw the notification as appropriate, depending on the seriousness of the failure. It shall also immediately inform the Commission and the other Member States accordingly.

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

Article 37
Challenge to the competence of notified bodies

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

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

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

4. Where the Commission ascertains that a notified body does not meet or no longer meets the requirements ***for its notification***, it shall ***inform*** the notifying Member State ***accordingly and request it*** to take the necessary corrective measures, including ***suspension or*** withdrawal of ***the*** notification if necessary. ***Where the Member State fails to take the necessary corrective measures, the Commission may, by means of an implementing act, suspend, restrict or withdraw the designation.*** That implementing act shall be adopted in accordance with the examination procedure referred to in Article 74(2).

Article 38
Coordination of notified bodies

1. The Commission shall ensure that, with regard to the areas covered by this Regulation, appropriate coordination and cooperation between notified bodies active in the conformity assessment procedures of AI systems pursuant to this Regulation are put in place and properly operated in the form of a sectoral group of notified bodies**.**

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

2a. The Commission shall provide for the exchange of knowledge and best practices between the Member States' national authorities responsible for notification policy.

Article 39
Conformity assessment bodies of third countries

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

(61) 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[1] should be a means for providers to demonstrate conformity with the requirements of this Regulation. ***To ensure the effectiveness of standards as policy tool for the Union and considering the importance of standards for ensuring conformity with the requirements of this Regulation and for the competitiveness of undertakings, it is necessary to ensure a balanced representation of interests by involving all relevant stakeholders in the development of standards. The standardisation process should be transparent in terms of legal and natural persons participating in the standartisation activities.***

(61b) In order to facilitate compliance, the first standardisation requests should be issued by the Commission two months after -the entry into force of this Regulation at the latest. This should serve to improve legal certainty, thereby promoting investment and innovation in AI, as well as competitiveness and growth of the Union market, while enhancing multistakeholder governance representing all relevant European stakeholders such as the AI Office, European standardisation organisations and bodies or experts groups established under relevant sectorial Union law as well as industry, SMEs, start-ups, civil society, researchers and social partners, and should ultimately facilitate global cooperation on standardisation in the field of AI in a manner consistent with Union values. When preparing the standardisation request, the Commission should consult the AI Office and the AI Advisory Forum in order to collect relevant expertise.

(61c) When AI systems are intended to be used at the workplace, harmonised standards should be limited to technical specifications and procedures.

(61d) The Commission should be able to adopt common specifications under certain conditions, when no relevant harmonised standard exists or to address specific fundamental rights concerns. Through the whole drafting process, the Commission should regularly consult the AI Office and its advisory forum, the European standardisation organisations and bodies or expert groups established under relevant sectorial Union law as well as relevant stakeholders, such as industry, SMEs, start-ups, civil society, researchers and social partners.

(61e) When adopting common specifications, the Commission should strive for regulatory alignment on AI with likeminded global partners is key to fostering innovation and cross-border partnerships within the field of AI, as coordination with likeminded partners in international standardisation bodies is of great importance.

(62) 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. ***To increase the trust in the value chain and to give certainty to***

[1] 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 (OJ L 316, 14.11.2012, p. 12).

businesses about the performance of their systems, third-parties that supply AI components may voluntarily apply for a third-party conformity assessment.

(63) It is appropriate that, in order to minimise the burden on operators and avoid any possible duplication, for high-risk AI systems related to products which are covered by existing Union harmonisation legislation following the New Legislative Framework approach, the compliance of those AI systems with the requirements of this Regulation should be assessed as part of the conformity assessment already foreseen under that legislation. The applicability of the requirements of this Regulation should thus not affect the specific logic, methodology or general structure of conformity assessment under the relevant specific New Legislative Framework legislation. This approach is fully reflected in the interplay between this Regulation and the [Machinery Regulation]. While safety risks of AI systems ensuring safety functions in machinery are addressed by the requirements of this Regulation, certain specific requirements in the [Machinery Regulation] will ensure the safe integration of the AI system into the overall machinery, so as not to compromise the safety of the machinery as a whole. The [Machinery Regulation] applies the same definition of AI system as this Regulation.

(64) ***Given the complexity of high-risk AI systems and the risks that are associated to them, it is essential to develop a more adequate capacity for the application of third party conformity assessment for high-risk AI systems. However,*** given the ***current*** experience of professional pre-market certifiers in the field of product safety and the different nature of risks involved, it is appropriate to limit, at least in an initial phase of application of this Regulation, the scope of application of third-party conformity assessment for high-risk AI systems other than those related to products. Therefore, the conformity assessment of such systems should be carried out as a general rule by the provider under its own responsibility, with the only exception of AI systems intended to be used for the remote biometric identification of persons, ***or AI systems intended to be used to make inferences about personal characteristics of natural persons on the basis of biometric or biometrics-based data, including emotion recognition systems*** for which the involvement of a notified body in the conformity assessment should be foreseen, to the extent they are not prohibited.

(66) In line with the commonly established notion of substantial modification for products regulated by Union harmonisation legislation, it is appropriate that an ***high-risk*** AI system undergoes a new conformity assessment whenever a***n unplanned*** change occurs ***which goes beyond controlled or predetermined changes by the provider including continuous learning and*** which may ***create a new unacceptable risk and significantly*** affect the compliance of the ***high-risk AI*** system with this Regulation or when the intended purpose of the system changes. In addition, as regards 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), it is necessary to provide rules establishing that changes to the algorithm and its performance that have been pre-determined by the provider and assessed at the moment of the conformity assessment should not constitute a substantial modification. ***The same should apply to updates of the AI system for security reasons in general and to protect against evolving threats of manipulation of the system, as lond as they do not amount to a substantial modification.***

(67) High-risk AI systems should bear the CE marking to indicate their conformity with this Regulation so that they can move freely within the internal market. ***For physical high-risk AI systems, a physical CE marking should be affixed, and may be complemented***

by a digital CE marking. For digital only high-risk AI systems, a digital CE marking should be used. Member States should not create unjustified obstacles to the placing on the market or putting into service of high-risk AI systems that comply with the requirements laid down in this Regulation and bear the CE marking.

(68) Under certain conditions, rapid availability of innovative technologies may be crucial for health and safety of persons***, the environment and climate change*** and for society as a whole. It is thus appropriate that under exceptional reasons of protection of life and health of natural persons, ***environmental protection*** and the protection of ***critical infrastructure***, Member States could authorise the placing on the market or putting into service of AI systems which have not undergone a conformity assessment.

(69) 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 towards the public, providers of high-risk AI systems other than those related to products falling within the scope of relevant existing Union harmonisation legislation, should be required to register their high-risk AI system ***and foundation models*** in a EU database, to be established and managed by the Commission. ***This database should be freely and publicly accessible, easily understandable and machine-readable. The database should also be user-friendly and easily navigable, with search functionalities at minimum allowing the general public to search the database for specific high-risk systems, locations, categories of risk under Annex IV and keywords. Deployers who are public authorities or European Union institutions, bodies, offices and agencies or deployers acting on their behalf and deployers who are undertakings designated as a gatekeeper under Regulation 2022/1925 should also register in the EU database before putting into service or using a high-risk AI system for the first time and following each substantial modification. Other deployers should be entitled to do so voluntarily. Any substantial modification of high-risk AI systems shall also be registered in the EU database.*** The Commission should be the controller of that database, in accordance with Regulation (EU) 2018/1725 of the European Parliament and of the Council[2]. 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. ***The Commission should take into account cybersecurity and hazard-related risks when carrying out its tasks as data controller on the EU database. In order to maximise the availability and use of the database by the public, the database, including the information made available through it, should comply with requirements under the European Accessibility Act.***

CHAPTER 5

STANDARDS, CONFORMITY ASSESSMENT, CERTIFICATES, REGISTRATION

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

Article 40
Harmonised standards

1. High-risk AI systems ***and foundation models*** which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union ***in accordance with Regulation 1025/2012 (AM 2122)*** shall be presumed to be in conformity with the requirements set out in Chapter 2 of this Title ***or Article 28b***, to the extent those standards cover those requirements.

1a. The Commission shall issue standardisation requests covering all requirements of this Regulation, in accordance with Article 10 of Regulation 1025/2012 no later than 2 months after the date of entry into force of this Regulation. When preparing standardisation request, the Commission shall consult the AI Office and the Advisory Forum.

1b. When issuing a standardisation request to European standardisation organisations, the Commission shall specify that standards shall be coherent, including with sectorial legislation listed in Annex II, and aimed at ensuring that AI systems or foundation models placed on the market or put into service in the Union meet the relevant requirements laid down in this Regulation;

1c. The actors involved in the standardisation process shall take into account the general principles for trustworthy AI set out in Article 4(a), seek to promote investment and innovation in AI as well as competitiveness and growth of the Union market, and contribute to strengthening global cooperation on standardisation and taking into account existing international standards in the field of AI that are consistent with Union values, fundamental rights and interests, and ensure a balanced representation of interests and effective participation of all relevant stakeholders in accordance with Articles 5, 6, and 7 of Regulation (EU) No 1025/2012.

Article 41
Common specifications

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

1a. The Commission may, by means of implementing act adopted in accordance with the examination procedure referred to in Article 74(2) and after consulting the AI Office and the AI Advisory Forum, adopt common specifications in respect of the requirements set out in Chapter 2 of this Title or Article 28b when the following conditions are fulfilled:

(a) there is no reference to harmonised standards already published in the Official Journal of the European Union related to the essential requirement(s), unless the harmonised standard in question is an existing standard that must be revised; and

(b) the Commission has requested one or more European standardisation organisations to draft a harmonised standard for the essential requirement(s) set out in Chapter 2; and

(c) the request referred to in point (b) has not been accepted by any of the European standardisation organisations; or there are undue delays in the establishment of an appropriate harmonised standard; or the standard provided does not satisfy the requirements of the relevant EU legislation, or does not comply with the request of the Commission.

1b. Where the Commission considers there is a need to adress specific fundamental rights concerns, common specifications adopted by the Commission in accordance with paragraph 1 shall also address those specific fundamental rights concerns.

1c. The Commission shall develop common specifications for the methodology to fulfil the reporting and documentation requirement on the consumption of energy and resources during development, training and deployment of the high risk AI system

2. The Commission, ***throughout the whole process of drafting*** the common specifications referred to in paragraph***s 1a and 1b***, shall ***regularly consult the AI Office and the Advisory Forum, the European standardisation organisations and*** bodies or expert groups established under relevant sectorial Union law ***as well as other relevant stakeholders,*** ~~bodies or expert groups established under relevant sectorial Union law~~. ***The Commission shall fulfil the objectives referred to in Article 40 (1c) and duly justify why it decided to resort to common specifications. Where the Commission intends to adopt common specifications pursuant to paragraph 1b of this Article, it shall also clearly identify the specific fundamental rights concern to be addressed.***

When adopting common specifications pursuant to paragraphs 1a and 1b of this Article, the Commission shall take into account the opinion issued by the AI Office referred to in Article 56e(b) of this Regulation. Where the Commission decides not to follow the opinion of the AI Office, it shall provide a reasoned explanation to the AI Office.

3. High-risk AI systems which are in conformity with the common specifications referred to in paragraph ***1a and 1b*** shall be presumed to be in conformity with the requirements set out in Chapter 2 of this Title, to the extent those common specifications cover those requirements

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

4. Where providers ***of high-risk AI systems*** do not comply with the common specifications referred to in paragraph 1, they shall duly justify that they have adopted technical solutions that ***meet the requirements referred to in Chapter II to a level*** at least equivalent thereto.

Article 42
Presumption of conformity with certain requirements

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

2. High-risk AI systems that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 of the European Parliament and of the Council[3] and the references of which have been published in the Official Journal of the European Union shall be presumed to be in compliance with the cybersecurity requirements set out in Article 15 of this Regulation in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements.

Article 43
Conformity assessment

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

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

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

In demonstrating the compliance of a high-risk AI system with the requirements set out in Chapter 2 of this Title, the provider ***shall follow the conformity assessment procedure set out in Annex VII in the following cases:***

   (a) where harmonised standards referred to in Article 40, the reference number of which has been published in the Official Journal of the European Union, covering all relevant safety requirements for the AI system, do not exist and common specifications referred to in Article 41 are not available;

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

(b) where the technical specifications referred to in point (a) exist but the provider has not applied them or has applied them only in part;

(c) where one or more of the technical specifications referred to in point (a) has been published with a restriction and only on the part of the standard that was restricted;

(d) when the provider considers that the nature, design, construction or purpose of the AI system necessitate third party verification, regardless of its risk level..

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

2. For high-risk AI systems referred to in points 1 to 8 of Annex III, providers shall follow the conformity assessment procedure based on internal control as referred to in Annex VI, which does not provide for the involvement of a notified body. For high-risk AI systems referred to in point 5(b) of Annex III, placed on the market or put into service by credit institutions regulated by Directive 2013/36/EU, the conformity assessment shall be carried out as part of the procedure referred to in Articles 97 to 101 of that Directive.

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

   For the purpose of that assessment, notified bodies which have been notified under those legal acts shall be entitled to control the conformity of the high-risk AI systems with the requirements set out in Chapter 2 of this Title, provided that the compliance of those notified bodies with requirements laid down in Article 33(4), (9) and (10) has been assessed in the context of the notification procedure under those legal acts.

   Where the legal acts listed in Annex II, section A, enable the manufacturer of the product to opt out from a third-party conformity assessment, provided that that manufacturer has applied all harmonised standards covering all the relevant requirements, that manufacturer may make use of that option only if he has also applied harmonised standards or, where applicable, common specifications referred to in Article 41, covering the requirements set out in Chapter 2 of this Title.

4. High-risk AI systems ***that have already been subject to a conformity assessment procedure*** shall undergo a new conformity assessment procedure whenever they are substantially modified, regardless of whether the modified system is intended to be further distributed or continues to be used by the current ***deployer.***

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

4 a. ***The specific interests and needs of SMEs shall be taken into account when setting the fees for third-party conformity assessment under this Article, reducing those fees proportionately to their size and market share.***

5. The Commission is empowered to adopt delegated acts in accordance with Article 73 for the purpose of updating Annexes VI and Annex VII in order to introduce elements of the conformity assessment procedures that become necessary in light of technical progress. ***In doing so, the Commission shall consult the AI Office and the affected stakeholders***

6. The Commission is empowered to adopt delegated acts to amend paragraphs 1 and 2 in order to subject high-risk AI systems referred to in points 2 to 8 of Annex III to the conformity assessment procedure referred to in Annex VII or parts thereof. The Commission shall adopt such delegated acts taking into account the effectiveness of the conformity assessment procedure based on internal control referred to in Annex VI in preventing or minimizing the risks to health and safety and protection of fundamental rights posed by such systems as well as the availability of adequate capacities and resources among notified bodies. ***In doing so, the Commission shall consult the AI Office and the affected stakeholders.***

Article 44
Certificates

1. Certificates issued by notified bodies in accordance with Annex VII shall be drawn-up in ***one or several*** official Union language***s*** determined by the Member State in which the notified body is established or in ***one or several*** official Union language***s*** otherwise acceptable to the notified body.

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

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

Article 45
Appeal against decisions of notified bodies

Member States shall ensure that an appeal procedure against decisions of the notified bodies, ***including on issued conformity certificates*** is available to parties having a legitimate interest in that decision.

Article 46
Information obligations of notified bodies

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

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

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

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

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

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

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

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

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

3. Each notified body shall provide the other notified bodies 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 47

Derogation from conformity assessment procedure

1. By way of derogation from Article 43, any ***national supervisory authority may request a judicial authority to*** authorise the placing on the market or putting into service of specific high-risk AI systems within the territory of the Member State concerned, for exceptional reasons of ~~public security or~~ the protection of life and health of persons, environmental protection and the protection of ***critical infrastructure***. That authorisation shall be for a limited period of time, while the necessary conformity assessment procedures are being carried out, and shall terminate once those procedures have been completed. The completion of those procedures shall be undertaken without undue delay.

2. The authorisation referred to in paragraph 1 shall be issued only if the ***national supervisory*** authority ***and judicial authority*** conclude~~s~~ that the high-risk AI system complies with the requirements of Chapter 2 of this Title. The ***national supervisory*** authority shall inform the Commission, ***the AI office,*** and the other Member States of any ***request made and any subsequent*** authorisation issued pursuant to paragraph 1.

3. Where, within 15 calendar days of receipt of the information referred to in paragraph 2, no objection has been raised by either a Member State or the Commission in respect ***to the request of the national supervisory authority for*** an authorisation issued by a

national supervisory authority of a Member State in accordance with paragraph 1, that authorisation shall be deemed justified.

4. Where, within 15 calendar days of receipt of the notification referred to in paragraph 2, objections are raised by a Member State against ***a request*** issued by a ***national supervisory*** authority of another Member State, or where the Commission considers the authorisation to be contrary to Union law or the conclusion of the Member States regarding the compliance of the system as referred to in paragraph 2 to be unfounded, the Commission shall without delay enter into consultation with the relevant Member State ***and the AI Office***; the operator(s) concerned shall be consulted and have the possibility to present their views. In view thereof, the Commission shall decide whether the authorisation is justified or not. The Commission shall address its decision to the Member State concerned and the relevant operator***(s)*** ~~or operators~~

5. If the authorisation is considered unjustified, this shall be withdrawn by the ***national supervisory*** authority of the Member State concerned.

6. By way of derogation from paragraphs 1 to 5, 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 apply also with regard to the derogation from the conformity assessment of the compliance with the requirements set out in Chapter 2 of this Title.

Article 48
EU declaration of conformity

1. The provider shall draw up a written ***machine readable, physical or electronic*** EU declaration of conformity for each ***high-risk*** AI system and keep it at the disposal of the national ***supervisory authority and the national*** competent authorities for 10 years after the AI ***high-risk*** system has been placed on the market or put into service**.** A copy of the EU declaration of conformity shall be ~~–~~***submitted*** to the ***national supervisory authority and the*** relevant national competent authorities upon request.

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

3. Where high-risk AI systems are subject to other Union harmonisation legislation which also requires an EU declaration of conformity, a single EU declaration of conformity ***may*** 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.

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

5. ***After consulting the AI office,*** the Commission shall be empowered to adopt delegated acts in accordance with Article 73 for the purpose of updating the content of the EU declaration of conformity set out in Annex V in order to introduce elements that become necessary in light of technical progress.

Article 49
CE marking of conformity

1. The ***physical*** CE marking shall be affixed visibly, legibly and indelibly for high-risk AI systems ***before the high-risk AI system is placed on the market***. Where that is not possible or not warranted on account of the nature of the high-risk AI system, it shall be affixed to the packaging or to the accompanying documentation, as appropriate. ***It may be followed by a pictogram or any other marking indicating a special risk of use.***

1a. For digital only high-risk AI systems, a digital CE marking shall be used, only if it can be easily accessed via the interface from which the artificial intelligence system is accessed or via an easily accessible machine-readable code or other electronic means.

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 43. The identification number ***of the notified body shall be affixed by the body itself or, under its instructions, by the provider's authorised representative. The identification number*** shall also be indicated in any promotional material which mentions that the high-risk AI system fulfils the requirements for CE marking.

3a. Where high-risk AI systems are subject to other Union legislation which also provides for the affixing of the CE marking, the CE marking shall indicate that the high-risk AI system also fulfil the requirements of that other legislation.

Article 50
Document retention

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

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

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

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

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

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

Article 51
Registration

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

1a. Before putting into service or using a high-risk AI system in accordance with Article 6(2), the following categories of deployers shall register the use of that AI system in the EU database referred to in Article 60:

a) deployers who are public authorities or Union institutions, bodies, offices or agencies or deployers acting on their behalf
b)–deployers who are undertakings designated as a gatekeeper under Regulation 2022/1925;

1b. Deployers who do not fall under subparagraph 1a. shall be entitled to voluntarily register the use of a high-risk AI system referred to in Article 6(2) in the EU database referred to in Article 60;

1c. An updated registration entry must be completed immediately following each substantial modification.

ANNEX V
EU DECLARATION OF CONFORMITY

The EU declaration of conformity referred to in Article 48, 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;

4a. Where an AI system involves the processing of personal data, a statement that that AI system complies with Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680.

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;

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

ANNEX VI
CONFORMITY ASSESSMENT PROCEDURE BASED ON INTERNAL CONTROL

1. The conformity assessment procedure based on internal control is the conformity assessment procedure based on points 2 to 4.

2. The provider verifies that the established quality management system is in compliance with the requirements of Article 17.

3. The provider examines the information contained in the technical documentation in order to assess the compliance of the AI system with the relevant essential requirements set out in Title III, Chapter 2.

4. The provider also verifies that the design and development process of the AI system and its post-market monitoring as referred to in Article 61 is consistent with the technical documentation.

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

1. Introduction

Conformity based on assessment of quality management system and assessment of the technical documentation is the conformity assessment procedure based on points 2 to 5.

2. Overview

The approved quality management system for the design, development and testing of AI systems pursuant to Article 17 shall be examined in accordance with point 3 and shall be subject to surveillance 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 application of the provider 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;

(c) the technical documentation for each AI system covered under the same quality management system;

(d) the documentation concerning the quality management system which shall cover all the aspects listed under Article 17;

(e) a description of the procedures in place to ensure that the quality management system remains adequate and effective;

(f) a written declaration that the same application has not been lodged with any other notified body.

3.2. The quality management system shall be assessed by the notified body, which shall determine whether it satisfies the requirements referred to in Article 17.

The decision shall be notified to the provider or its authorised representative.

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

3.3. The quality management system as approved shall continue to be implemented and maintained by the provider so that it remains adequate and efficient.

3.4. Any intended change to the approved quality management system or the list of AI systems covered by the latter shall be brought to the attention of the notified body by the provider.

The proposed changes shall be examined by the notified body, which shall decide whether the modified quality management system continues to satisfy the requirements referred to in point 3.2 or whether a reassessment is necessary.

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

4. Control of the technical documentation.

4.1. In addition to the application referred to in point 3, an application with a notified body of their choice shall be lodged by the provider for the assessment of the technical documentation relating to the AI system which the provider 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:

(a) the name and address of the provider;

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

(c) the technical documentation referred to in Annex IV.

4.3. The technical documentation shall be examined by the notified body. To this purpose, 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 technical documentation, 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 set out in Title III, Chapter 2. 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.

4.5. Where necessary to assess the conformity of the high-risk AI system with the requirements set out in Title III, Chapter 2***, after all other reasonable ways to verify conformity have been exhausted and have proven to be insufficient,*** and upon a reasoned request, the notified body shall also be granted access to the ***training and trained models*** of the AI system, ***including its relevant parameters***. ***Such access shall***

be subject to existing Union law on the protection of intellectual property and trade secrets. They shall take technical and organisational measures to ensure the protection of intellectual property and trade secrets.

4.6. The decision shall be notified to the provider or its authorised representative. The notification shall contain the conclusions of the assessment of the technical documentation and the reasoned assessment decision.

Where the AI system is in conformity with the requirements set out in Title III, Chapter 2, an EU technical documentation assessment certificate shall be issued by the notified body. 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 set out in Title III, Chapter 2, 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, notably on the reasons for non-compliance.

4.7. Any change to the AI system that could affect the compliance of the AI system with the requirements 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 or if it becomes otherwise aware of the occurrence of such changes. The intended changes shall be assessed by the notified body which shall decide whether those changes require a new conformity assessment in accordance with Article 43(4) 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.

5. Surveillance of the approved quality management system.

5.1. The purpose of the surveillance carried out by the notified body referred to in Point 3 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. The provider shall further share with the notified body all necessary information.

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.

ANNEX VIII
INFORMATION TO BE SUBMITTED UPON THE REGISTRATION OF HIGH-RISK AI SYSTEMS IN ACCORDANCE WITH ARTICLE 51

Section A - 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 ***51 (1).***

1. Name, address and contact details of the provider;
2. Where submission of information is carried out by another person on behalf of the provider, the name, address and contact details of that person;
3. Name, address and contact details of the authorised representative, where applicable;
4. AI system trade name and any additional unambiguous reference allowing identification and traceability of the AI system;

4a. Foundation model trade name and any additional unambiguous refernce allowing identification and traceability

5. ***A simple and comprehensible*** description of
   a. the intended purpose of the AI system;
   b. ***the components and functions supported through AI***
   c. ***a basic explanation of the logic of the AI system***

5a. where applicable, the categories and nature of data likely or foreseen to be processed by the AI system;

6. Status of the AI system (on the market, or in service; no longer placed on the market/in service, recalled);
7. Type, number and expiry date of the certificate issued by the notified body and the name or identification number of that notified body, when applicable;
8. A scanned copy of the certificate referred to in point 7, when applicable;
9. Member States in which the AI system is or has been placed on the market, put into service or made available in the Union;
10. A copy of the EU declaration of conformity referred to in Article 48;
11. ~~Electronic instructions for use; this information shall not be provided for high-risk AI systems in the areas of law enforcement and migration, asylum and border control management referred to in Annex III, points 1, 6 and 7.~~
12. URL for additional information (optional).

SECTION B - 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 51 (1a(a) and (1b)

1. ***the name, address and contact details of the deployer***
2. ***the name, address and contact details of the person submitting information on behalf of the deployer***

3. ***the high-risk AI system trade name and any additional unambiguous reference allowing identification and traceability of the AI system used***
4. ***a. A simple and comprehensible description of the intended use of the AI system, including the specific outcomes sought through the use of the systemn, the geographic and temporal scope of application***
   b. Where applicable, the categories and nature of data to be processed by the AI system;
   c. Arrangements for human oversight and governance
   d. Where relevant, the bodies or natural persons responsible for decisions taken or supported by the AI system.
5. ***a summary of the findings of the fundamental rights impact assessment conducted in accordance with Article 29a***
6. ***The URL of the entry of the AI system in the EU database by its provider***
7. ***a summary of the data protection impact assessment carried out in accordance with Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680 as specified in paragraph 6 of Article 29 of this Regulation, where applicable***

Section C - ***The following information shall be provided and thereafter kept up to date with regard to foundation models to be registered in accordance with Article 28b (e).***

1. ***Name, address and contact details of the provider;***
2. ***Where submission of information is carried out by another person on behalf of the provider, the name, address and contact details of that person;***
3. ***Name, address and contact details of the authorised representative, where applicable;***
4. ***Trade name and any additional unambiguous reference allowing the identificationof the foundation model***
5. ***Description of the data sources used in the developmentof the foundational model***
6. ***Description of the capabilities and limitations of the foundation model, including the reasonably foreseeable risks and the measures that have been taken to mitigate them as well as remaining non-mitigated risks with an explanation on the reason why they cannot be mitigated***
7. ***Description of the training resources used by the foundation model including computing power required, training time, and other relevant information related to the size and power of the model***
8. ***Description of the model's performance, including on public benchmarks or state of the art industry benchmarks***
9. ***Description of the results of relevant internal and external testing and optimisation of the model 10. Member States in which the foundation model is or has been placed on the market,***

put into service or made available in the Union;

11. URL for additional information (optional).

Articles 16 to 29a and associated recitals	**CA 3**

(53) It is appropriate that a specific natural or legal person, defined as the provider, takes 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 is the person who designed or developed the system.

(53a) As signatories to the United Nations Convention on the Rights of Persons with Disabilities (UNCRPD), the European Union and all Member States are legally obliged to protect persons with disabilities from discrilmination and promote their equality, to ensure that persons with disabilities have access, on an equal basis wirh others, to information and communications technologies and systems, and to ensure respect for privacy for persons with disabilities. Given the growing importance and use of AI systems, the application of universal design principles to all new technologies and services should ensure full, equal, and unrestricted access for everyone potentially affected by or using AI technologies, including persons with disabilities, in a way that takes full account of their inherent dignity and diversity. It is therefore essential that Providers ensure full compliance with accessibility requirements, including Directive 2019/882 and Directive 2016/2102 of the European Parliament and of the Council. Providers should ensure compliance with these requirements by design. Therefore, the necessary measures should be integrated as much as possible into the design of the high-risk AI system.

(54) The provider should establish a sound quality management system, ensure the accomplishment of the required conformity assessment procedure, draw up the relevant documentation and establish a robust post-market monitoring system. ***For providers that have already in place quality management systems based on standards such as ISO 9001 or other relevant standards, no duplicative quality management system in full should be expected but rather an adaptation of their existing systems to certain aspects linked to compliance with specific requirements of this Regulation. This should also be reflected in future standardization activities or guidance adopted by the Commission in this respect.*** Public authorities which put into service high-risk AI systems for their own use may adopt and implement the rules for the quality management system as part of the quality management system adopted at a national or regional level, as appropriate, taking into account the specificities of the sector and the competences and organisation of the public authority in question.

(55) Where a high-risk AI system that is a safety component of a product which is covered by a relevant New Legislative Framework sectorial legislation is not placed on the market or put into service independently from the product, the manufacturer of the final product as 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 embedded in the final product complies with the requirements of this Regulation.

(56) To enable enforcement of this Regulation and create a level-playing field for operators, and taking into account the different forms of making available of digital products, it is important to ensure that, under all circumstances, a person established in the Union can provide authorities with all the necessary information on the compliance of an AI system. Therefore, prior to making their AI systems available in the Union ~~where an importer cannot be identified~~, providers established outside the Union shall, by written mandate, appoint an authorised representative established in the Union.

(57) 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.

(58) Given the nature of AI systems and the risks to safety and fundamental rights possibly associated with their use, including as ***regards*** the need to ensure proper monitoring of the performance of an AI system in a real-life setting, it is appropriate to set specific responsibilities for ***deployers***. ***Deployers*** should in particular use high-risk AI systems in accordance with the instructions of use and certain other obligations should be provided for with regard to monitoring of the functioning of the AI systems and with regard to record-keeping, as appropriate.

(***58 a) Whilst risks related to AI systems can result from the way such systems are designed, risks can as well stem from how such AI systems are used. Deployers of high-risk AI system therefore play a critical role in ensuring that fundamental rights are protected, complementing the obligations of the provider when developing the AI system. Deployers are best placed to understand how the high-risk AI system will be used concretely and can therefore identify potential significant risks that were not foreseen in the development phase, due to a more precise knowledge of the context of use, the people or groups of people likely to be affected, including marginalised and vulnerable groups. Deployers should identify appropriate governance structures in that specific context of use, such as arrangements for human oversight, complaint-handling procedures and redress procedures, because choices in the governance structures can be instrumental in mitigating risks to fundamental rights in concrete use-cases. In order to efficiently ensure that fundamental rights are protected, the deployer of high-risk AI systems should therefore carry out a fundamental rights impact assessment prior to putting it into use. The impact assessment should be accompanied by a detailed plan describing the measures or tools that will help mitigating the risks to fundamental rights identified at the latest from the time of putting it into use. If such plan cannot be identified, the deployer should refrain from putting the system into use. When performing this impact assessment, the deployer should notify the national supervisory authority and, to the best extent possible relevant stakeholders as well as representatives of groups of persons likely to be affected by the AI system in order to collect relevant information which is deemed necessary to perform the impact assessment and are encouraged to make the summary of their fundamental rights impact assessment publicly available on their online website. This obligations should not apply to SMEs which, given the lack of resrouces, might find it difficult to perform such consultation.Nevertheless, they should also strive to invole such representatives when carrying out their fundamental rights impact assessment.In addition, given the potential impact and the need for democratic oversight and scrutiny, deployers of high-risk AI systems that are public authorities or Union institutions, bodies, offices and agencies, as well deployers who are undertakings designated as a gatekeeper under Regulation 2022/1925 should be required to register the use of any high-risk AI system in a public database. Other deployers may voluntarily register.***

(59) It is appropriate to envisage that the ***deployer*** of the AI system should be the natural or legal person, public authority, agency or other body under whose authority the AI system is operated except where the use is made in the course of a personal non-professional activity.

(60) ***Within the AI value chain multiple entities often supply tools and services but also components or processes that are then incorporated by the provider into the AI system, including in relation to data collection and pre-processing, model training, model retraining, model testing and evaluation, integration into software, or other aspects of model development. The involved entities may make their offering commercially available directly or indirectly, through interfaces, such as Application Programming Interfaces (API), and distributed under free and open source licenses but also more and more by AI workforce platforms, trained parameters resale, DIY kits to build models or the offering of paying access to a model serving architecture to develop and train models.*** In the light of this complexity of the AI value chain, ***all relevant third parties, notably those that are involved in the development,*** sale and the commercial supply of software tools, components, pre-trained models or data incorporated into the AI system, or providers of network services, ***should without compromising their own intellectual property rights or trade secrets, make available the required information, training or expertise and*** cooperate, as appropriate, with providers to enable their ***control over all compliance relevant aspects of the AI system that falls*** under this Regulation. ***To allow a cost-effective AI value chain governance, the level of control shall be explicitly disclosed by each third party that supplies the provider with a tool, service, component or process that is later incorporated by the provider into the AI system.***

(60a) ***Where one party is in a stronger bargaining position, there is a risk that that party could leverage such position to the detriment of the other contracting party when negotiating the supply of tools, services, components or processes that are used or integrated in a high risk AI system or the remedies for the breach or the termination of related obligations. Such contractual imbalances particularly harm micro, small and medium-sized enterprises as well as start-ups, unless they are owned or sub-contracted by an enterprise which is able to compensate the sub-contractor appropriately, as they are without a meaningful ability to negotiate the conditions of the contractual agreement, and may have no other choice than to accept 'take-it-or-leave-it' contractual terms. Therefore, unfair contract terms regulating the supply of tools, services, components or processes that are used or integrated in a high risk AI system or the remedies for the breach or the termination of related obligations should not be binding to such micro, small or medium-sized enterprises and start-ups when they have been unilaterally imposed on them.***

(60b) Rules on contractual terms should take into account the principle of contractual freedom as an essential concept in business-to-business relationships. Therefore, not all contractual terms should be subject to an unfairness test, but only to those terms that are unilaterally imposed on micro, small and medium-sized enterprises and start-ups. This concerns 'take-it-or-leave-it' situations where one party supplies a certain contractual term and the micro, small or medium-sized enterprise and start-up cannot influence the content of that term despite an attempt to negotiate it. A contractual term that is simply provided by one party and accepted by the micro, small, medium-sized enterprise or a start-up or a term that is negotiated and subsequently agreed in an amended way between contracting parties should not be considered as unilaterally imposed.

(60c) Furthermore, the rules on unfair contractual terms should only apply to those elements of a contract that are related to supply of tools, services, components or

processes that are used or integrated in a high risk AI system or the remedies for the breach or the termination of related obligations. Other parts of the same contract, unrelated to these elements, should not be subject to the unfairness test laid down in this Regulation.

(60d) Criteria to identify unfair contractual terms should be applied only to excessive contractual terms, where a stronger bargaining position is abused. The vast majority of contractual terms that are commercially more favourable to one party than to the other, including those that are normal in business-to-business contracts, are a normal expression of the principle of contractual freedom and continue to apply. If a contractual term is not included in the list of terms that are always considered unfair, the general unfairness provision applies. In this regard, the terms listed as unfair terms should serve as a yardstick to interpret the general unfairness provision.

(60e) Foundation models are a recent development, in which AI models are developed from algorithms designed to optimize for generality and versatility of output. Those models are often trained on a broad range of data sources and large amounts of data to accomplish a wide range of downstream tasks, including some for which they were not specifically developed and trained. Those systems can be unimodal or multimodal, trained through various methods such as supervised learning or reinforced learning. AI systems with specific intended purpose or general purpose AI systems can be an implementation of a foundation model, which means that each foundation model can be reused in countless downstream AI or general purpose AI systems. These models hold growing importance to many downstream applications and systems.

(60f) In the case of foundation models provided as a service such as through API access, the cooperation with downstream providers should extend throughout the time during which that service is provided and supported, in order to enable appropriate risk mitigation, unless the provider of the foundation model transfers the training model as well as extensive and appropriate information on the datasets and the development process of the system or restricts the service, such as the API access, in such a way that the downstream provider is able to fully comply with this Regulation without further support from the original provider of the foundation model.

(60g) In light of the nature and complexity of the value chain for AI system, it is essential to clarify the role of actors contributing to the development of AI systems. There is significant uncertainty as to the way foundation models will evolve, both in terms of typology of models and in terms of self-governance. Therefore, it is essential to clarify the legal situation of providers of foundation models. Combined with their complexity and unexpected impact, the downstream AI provider's lack of control over the foundation model's development and the consequent power imbalance and in order to ensure a fair sharing of responsibilities along the AI value chain, such models should be subject to proportionate and more specific requirements and obligations under this Regulation, namely foundation models should assess and mitigate possible risks and harms through appropriate design, testing and analysis, should implement data governance measures, including assessment of biases, and should comply with technical design requirements to ensure appropriate levels of performance, predictability, interpretability, corrigibility, safety and cybersecurity and should comply with environmental standards. These obligations should be accompanied by

standards. Also, foundation models should have information obligations and prepare all necessary technical documentation for potential downstream providers to be able to comply with their obligations under this Regulation. Generative foundation models should ensure transparency about the fact the content is generated by an AI system, not by humans. These specific requirements and obligations do not amount to considering foundation models as high risk AI systems, but should guarantee that the objectives of this Regulation to ensure a high level of protection of fundamental rights, health and safety, environment, democracy and rule of law are achieved. Pre-trained models developed for a narrower, less general, more limited set of applications that cannot be adapted for a wide range of tasks such as simple multi-purpose AI systems should not be considered foundation models for the purposes of this Regulation, because of their greater interpretability which makes their behaviour less unpredictable.

(60h) Given the nature of foundation models, expertise in conformity assessment is lacking and third-party auditing methods are still under development .–The sector itself is therefore developing new ways to assess fundamental models that fulfil in part the objective of auditing (such as model evaluation, red-teaming or machine learning verification and validation techniques). Those internal assessments for foundation models should be should be broadly applicable (e.g. independent of distribution channels, modality, development methods), to address risks specific to such models taking into account industry state-of-the-art practices and focus on developing sufficient technical understanding and control over the model, the management of reasonably foreseeable risks, and extensive analysis and testing of the model through appropriate measures, such as by the involvement of independent evaluators. As foundation models are a new and fast-evolving development in the field of artificial intelligence, it is appropriate for the Commission and the AI Office to monitor and periodically asses the legislative and governance framework of such models and in particular of generative AI systems based on such models, which raise significant questions related to the generation of-content in breach of Union law, copyright rules, and potential misuse.
It should be clarified that this Regulation should be without prejudice to Union law on copyright and related rights, including Directives 2001/29/EC, 2004/48/ECR and (EU) 2019/790 of the European Parliament and of the Council.
It should be clarified that this Regulation should be without prejudice to Union law on copyright and related rights, including Directives 2001/29/EC, 2004/48/ECR and (EU) 2019/790 of the European Parliament and of the Council.

CHAPTER 3

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

Obligations of providers ***anddeployers*** of high-risk AI systems ***and other parties***

Article 16
Obligations of providers of high-risk AI systems

Providers of high-risk AI systems shall:

(a) ensure that their high-risk AI systems are compliant with the requirements set out in Chapter 2 of this Title ***before placing them on the market or putting them into service***;

(aa) indicate their name, registered trade name or registered trade mark, and their address and contact information on the high-risk AI system or, where that is not possible, on its accompanying documentation, as appropriate;

(ab) ensure that natural persons to whom human oversight of high-risk AI systems is assigned are specifically made aware of the risk of automation or confirmation bias;

(ac) provide specifications for the input data, or any other relevant information in terms of the datasets used, including their limitation and assumptions, taking into account the intended purpose and the foreseeable and reasonably foreseeable misuses of the AI system;

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

(c) draw-up ***and keep*** the technical documentation of the high-risk AI system ***referred to in Article 11***;

(d) when under their control, keep the logs automatically generated by their high-risk AI systems ***that are required for ensuring and demonstrating compliance with this Regulation, in accordance with Article 20*** ;

(e) ensure that the high-risk AI system undergoes the relevant conformity assessment procedure, prior to its placing on the market or putting into service***, in accordance with Article 43***;

(ea) draw up an EU declaration of conformity in accordance with Article 48;

(eb) affix the CE marking to the high-risk AI system to indicate conformity with this Regulation, in accordance with Article 49;

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

(g) take the necessary corrective actions ***as referred to in Article 21 and provide information in that regard***~~, if the high-risk AI system is not in conformity with the requirements set out in Chapter 2 of this Title~~;

~~(h) inform the national competent authorities of the Member States in which they made the AI system available or put it into service and, where applicable, the notified body of the non-compliance and of any corrective actions taken~~

~~(i) to affix the CE marking to ***the*** high-risk AI ***system*** to indicate the conformity with this Regulation, in accordance with Article 49;~~

(j) upon ***a reasoned*** request of a national ***supervisory*** authority, demonstrate the conformity of the high-risk AI system with the requirements set out in Chapter 2 of this Title.

(k) ensure that the high-risk AI system complies with accessibility requirements.

Article 17
Quality management system

1. Providers of high-risk AI systems shall ***have*** a quality management system in place that ensures compliance with this Regulation. ***It*** shall be documented in a systematic and orderly manner in the form of written policies, procedures ***or*** instructions, and can ***be incorporated into an existing quality management system under sectoral legislation. It shall*** include at least the following aspects:

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

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

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

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

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

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

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

(h) the setting-up, implementation and maintenance of a post-market monitoring system, in accordance with Article 61;

(i) procedures related to the reporting of serious incidents and of malfunctioning in accordance with Article 62;

(j) the handling of communication with ***relevant*** competent authorities, including sectoral ones, ~~providing or supporting the access to data, notified bodies, other operators, customers or other interested parties~~

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

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

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

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

3. For providers that are credit institutions regulated by Directive 2013/36/ EU, the obligation to put a quality management system in place shall be deemed to be fulfilled by complying with the rules on internal governance arrangements, processes and mechanisms pursuant to Article 74 of that Directive. In that context, any harmonised standards referred to in Article 40 of this Regulation shall be taken into account.

~~*Article 18*~~
~~*Obligation to draw up technical documentation*~~

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

~~*2. Providers that are credit institutions regulated by Directive 2013/36/EU shall maintain the technical documentation as part of the documentation concerning internal governance, arrangements, processes and mechanisms pursuant to Article 74 of that Directive.*~~

~~*Article 19*~~
~~*Conformity assessment*~~

~~1. Providers of high-risk AI systems shall ensure that their systems undergo the relevant conformity assessment procedure in accordance with Article 43, prior to their placing on the market or putting into service. Where the compliance of the AI systems with the requirements set out in Chapter 2 of this Title has been demonstrated following that conformity assessment, the providers shall draw up an EU declaration of conformity in accordance with Article 48 and affix the CE marking of conformity in accordance with Article 49.~~

~~2. For high-risk AI systems referred to in point 5(b) of Annex III that are placed on the market or put into service by providers that are credit institutions regulated by Directive 2013/36/EU, the conformity assessment shall be carried out as part of the procedure referred to in Articles 97 to101 of that Directive.~~

Article 20
Automatically generated logs

1. Providers of high-risk AI systems shall keep the logs automatically generated by their high-risk AI systems, to the extent such logs are under their control ~~by virtue of a contractual arrangement with the user or otherwise by law~~. ***Without prejudice to applicable Union or national law,*** the logs shall be kept for a period ***of at least 6 months. The retention period shall be in accordance with industry standards and appropriate to*** the intended purpose of high-risk AI system ~~and applicable legal obligations under Union or national law.~~

2. Providers that are credit institutions regulated by Directive 2013/36/EU shall maintain the logs automatically generated by their high-risk AI systems as part of the documentation under Articles 74 of that Directive.

Article 21
Corrective actions

Providers of high-risk AI systems which consider or have reason to consider that a high-risk AI system which they have placed on the market or put into service is not in conformity with this Regulation shall immediately take the necessary corrective actions to bring that system into conformity, to withdraw it***, to disable 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.~~

1a. In the cases referred to in paragraph 1, providers shall immediately inform:

a. the distributors,
b. the importers,
c. the national competent authorities of the Member States in which they made the AI system available or put it into service; and
d. the deployer, where possible.

1b. The providers shall also inform the authorised representative, if one was appointed in accordance with Article 25, and the notified body if the high-risk AI system had to undergo a third-party conformity assessment in accordance with Article 43.
Where applicable, they shall also investigate the causes in collaboration with the deployer.

Article 22
Duty of information

1. Where the high-risk AI system presents a risk within the meaning of Article 65(1) and ~~that risk is known to~~ the provider of the system ***becomes aware of that risk,*** that provider shall immediately inform the national ***supervisory authorities*** of the Member States in which it made the system available and, where applicable, the notified body that issued a certificate for the high-risk AI system, in particular ***the nature*** of the non-compliance and of any ***relevant*** corrective actions taken.

1a. In the cases referred to in paragraph 1, providers of the high-risk AI system shall immediately inform:

a. the distributors,
b. the importers,
c. the national competent authorities of the Member States in which they made the AI system available or put it into service; and
d. the deployers, where possible,

1b. The providers shall also inform the authorised representative, if one was appointed in accordance with Article 25.

Article 23
*Cooperation with competent authorities**, the Office and the Commission***

Providers ***and where applicable, deployers*** of high-risk AI systems shall, upon ***a reasoned*** request by a national competent authority ***or where applicable, by the AI Office or the Commission,*** provide ***them*** with all the information and documentation necessary to demonstrate the conformity of the high-risk AI system with the requirements set out in Chapter 2 of this Title, in an official Union language determined by the Member State concerned. ~~Upon a reasoned request from a national competent authority, providers shall also give that authority access to the logs automatically generated by the high-risk AI system, to the extent such logs are under their control by virtue of a contractual arrangement with the user or otherwise by law~~

Upon a reasoned request by a national competent authority or, where applicable, by the Commission, providers and, where applicable, deployers shall also give the requesting national competent authority or the Commission, as applicable, access to the logs automatically generated by the high-risk AI system, to the extent such logs are under their control.

Any information obtained by a national competent authority or by the Commission pursuant to the provisions of this Article shall be considered a trade secret and be treated in compliance with the confidentiality obligations set out in Article 70.

Article 24
Obligations of product manufacturers

Where a high-risk AI system related to products to which the legal acts listed in Annex II, section A, apply, is placed on the market or put into service together with the product manufactured in accordance with those legal acts and under the name of the product manufacturer, the manufacturer of the product shall take the responsibility of the compliance of the AI system with this Regulation and, as far as the AI system is concerned, have the same obligations imposed by the present Regulation on the provider.

Article 25
Authorised representatives

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

1a. The authorised representative shall reside or be established in one of the Member States where the activities pursuant to Article 2, paragraphs 1(cb) are taking place.

1b. The provider shall provide its authorised representative with the necessary powers and resources to comply with its tasks under this Regulation.

2. The authorised representative shall perform the tasks specified in the mandate received from the provider. ***It shall provide a copy of the mandate to the market surveillance authorities upon request, in an official Union language determined by the national competent authority. For the purpose of this Regulation,*** the mandate shall empower the authorised representative to carry out the following tasks:

(a) ***ensure that*** the EU declaration of conformity and the technical documentation ***have been drawn up and that an appropriate conformity assessment procedure has been carried out by the provider***;

(aa) keep at the disposal of the national competent authorities and national authorities referred to in Article 63(7), a copy of the EU declaration of conformity, the technical documentation and, if applicable, the certificate issued by the notified body;

(b) provide a national competent authority, upon a reasoned request, with all the information and documentation necessary to demonstrate the conformity of a high-risk AI system with the requirements set out in Chapter 2 of this Title, including access to the logs automatically generated by the high-risk AI system to the extent such logs are under the control of the provider ~~by virtue of a contractual arrangement with the user or otherwise by law~~;

(c) cooperate with national ***supervisory*** authorities, upon a reasoned request, on any action the ***authority***-takes ***to reduce and mitigate the risks posed by the*** high-risk AI system.

(ca) where applicable, comply with the registration obligations referred in Article 51, or, if the registration is carried out by the provider itself, ensure that the information referred to in point 3 of Annex VIII is correct.

2a. The authorised representative shall be mandated to be addressed, in addition to or instead of the provider, by, in particular, national supervisory authority or the national competent authorities, on all issues related to ensuring compliance with this Regulation.

2b. The authorised representative shall terminate the mandate if it considers or has reasons to consider that the provider acts contrary to its obligations under this Regulation. In such a case, it shall also immediately inform the national supervisory authority of the Member State in which it is established, as well as, where applicable, the relevant notified body, about the termination of the mandate and the reasons thereof.

Article 26
Obligations of importers

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

(a) the ***relevant*** conformity assessment procedure ***referred to in Article 43*** has been carried out by the provider of that AI system

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

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

(ca) where applicable, the provider has appointed an authorised representative in accordance with Article 25(1).

2. Where an importer considers or has reason to consider that a high-risk AI system is not in conformity with this Regulation, ***or is counterfeit, or accompanied by falsified documentation*** it shall not place that system on the market until that AI system has been brought into conformity. Where the high-risk AI system presents a risk within the meaning of Article 65(1), the importer shall inform the provider of the AI system and the market surveillance authorities to that effect.

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

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

5. Importers shall provide national competent authorities, upon a reasoned request, with all ***the*** necessary information and documentation to demonstrate the conformity of a high-risk AI system with the requirements set out in Chapter 2 of this Title in a language which can be easily understood by ***them,*** including access to the logs automatically generated by the high-risk AI system to the extent such logs are under the control of the provider ***in accordance with Article 20.***

5a. Importers shall cooperate with national competent authorities on any action those authorities take to reduce and mitigate the risks posed by the high-risk AI system.

Article 27
Obligations of distributors

1. Before making a high-risk AI system available on the market, distributors shall verify that the high-risk AI system bears the required CE conformity marking, that it is accompanied by the required documentation and instruction of use, and that the provider and the importer of the system, as applicable, have complied with the***ir*** obligations set out in this Regulation ***in Article 16 and Article 26 respectively***.

2. Where a distributor considers or has reason to consider***, on the basis of the information in its possession*** that a high-risk AI system is not in conformity with the requirements set out in Chapter 2 of this Title, it shall not make the high-risk AI system available on the market until that system has been brought into conformity with those requirements. Furthermore, where the system presents a risk within the meaning of Article 65(1), the distributor shall inform the provider or the importer of the system, ***and the relevant national competent authority***, as applicable, to that effect

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

4. A distributor that considers or has reason to consider, ***on the basis of the information in its possession,*** that a high-risk AI system which it has made available on the market is not in conformity with the requirements set out in Chapter 2 of this Title shall take the corrective actions necessary to bring that system into conformity with those requirements, to withdraw it or recall it or shall ensure that the provider, the importer or any relevant operator, as appropriate, takes those corrective actions. Where the

high-risk AI system presents a risk within the meaning of Article 65(1), the distributor shall immediately inform ***the provider or importer of the system and*** the national competent authorities of the Member States in which it has made the product available to that effect, giving details, in particular, of the non-compliance and of any corrective actions taken.

5. Upon a reasoned request from a national competent authority, distributors of ***the*** high-risk AI system~~s~~ shall provide that authority with all the information and documentation ***in their possession or available to them, in accordance with the obligations of distributors as outlined in paragraph 1, that are*** necessary to demonstrate the conformity of a high-risk system with the requirements set out in Chapter 2 of this Title. ~~Distributors shall also cooperate with that national competent authority on any action taken by that authority~~.

5a. Distributors shall cooperate with national competent authorities on any action those authorities take to reduce and mitigate the risks posed by the high-risk AI system.

Article 28

Responsibilities along the AI value chain of providers, distributors, importers, deployers or other third party

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

   (a) they ***put their name or trademarkt on a high-risk AI system already placed*** on the market or put into service

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

   (ba) they make a substantial modification to an AI system, including a general purpose AI system, which has not been classified as high-risk and has already been placed on the market or put into service in such manner that the AI system becomes a high risk AI system in accordance with Article 6

2. Where the circumstances referred to in paragraph 1, point (***a***) ***to (ba)*** occur, the provider that initially placed the AI system on the market or put it into service shall no longer be considered a provider ***of that specific AI system*** for the purposes of this Regulation. ***This former provider shall provide the new provider with the technical documentation and all other relevant and reasonably expected information capabilities of the AI system, technical access or other assistance based on the generally acknowledged state of the art that are required for the fulfilment of the obligations set out in this Regulation.***

   Paragraph 2 shall also apply to providers of foundation models as defined in Article 3 when the foundation model is directly integrated in an high-risk AI system.

2a. The provider of a high risk AI system and the third party that supplies tools, services, components or processes that are used or integrated in the high risk AI system shall, by written agreement specify the information, capabilities, technical access, and or

other assistance, based on the generally acknowledged state of the art, that the third party must provide in order to enable the provider of the high risk AI system to fully comply with the obligations under this Regulation.

The Commission shall develop and recommend non-binding model contractual terms between providers of high-risk AI systems and third parties that supply tools, services, components or processes that are used or integrated in high-risk AI systems in order to assist both parties in drafting and negotiating contracts with balanced contractual rights and obligations, consistent with each party's level of control. When developing non-binding model contractual terms, the Commission shall take into account possible contractual requirements applicable in specific sectors or business cases. The non-binding contractual terms shall be published and be available free of charge in an easily usable electronic format on the AI Office's website.

2b. For the purposes of this Article, trade secrets shall be preserved and shall only be disclosed provided that all specific necessary measures pursuant to Directive (EU) 2016/943 are taken in advance to preserve their confidentiality, in particular with respect to third parties. Where necessary, appropriate technical and organizational arrangements can be agreed to protect intellectual property rights or trade secrets.

Article 28(a)
Unfair contractual terms unilaterally imposed on an SME or startup

1. A contractual term concerning the supply of tools, services, components or processes that are used or integrated in a high risk AI system or the remedies for the breach or the termination of related obligations which has been unilaterally imposed by an enterprise on a SME or start-up shall not be binding on the latter enterprise if it is unfair.

2. A contractual term is not to be considered unfair where it arises from applicable Union law.

3. A contractual term is unfair if it is of such a nature that it objectively impairs the ability of the party upon whom the term has been unilaterally imposed to protect its legitimate commercial interest in the information–in question or its use grossly deviates from good commercial practice in the supply of tools, services, components or processes that are used or integrated in a high-risk AI system, contrary to good faith and fair dealing or creates a significant imbalance between the rights and the obligations of the parties in the contract. A contractual term is also unfair if it has the effect of shifting penalties referred to in Article 71 or associated litigation costs across parties to the contract, as referred to in Article 71(8) (new).

4. A contractual term is unfair for the purposes of this Article if its object or effect is to:

(a) exclude or limit the liability of the party that unilaterally imposed the term for intentional acts or gross negligence;
(b) exclude the remedies available to the party upon whom the term has been unilaterally imposed in the case of non-performance of contractual

obligations or the liability of the party that unilaterally imposed the term in the case of a breach of those obligations;

(c) give the party that unilaterally imposed the term the exclusive right to determine whether the technical documentation, information supplied are in conformity with the contract or to interpret any term of the contract.

5. A contractual term shall be considered to be unilaterally imposed within the meaning of this Article if it has been supplied by one contracting party and the other contracting party has not been able to influence its content despite an attempt to negotiate it. The contracting party that supplied a contractual term bears the burden of proving that that term has not been unilaterally imposed.

6. Where the unfair contractual term is severable from the remaining terms of the contract, those remaining terms shall remain binding. The party that supplied the contested term may not argue that the term is an unfair term.

7. This Article shall apply to all new contracts entered into force after ... [date of entry into force of this Regulation]. Businesses shall be given three-years following that date to review existing contractual obligations that are subject to this Regulation.

8. Given the rapidity in which innovations occur in the markets, the list of unfair contractual terms within Article 28a shall be reviewed regularly by the Commission and be updated to new business practices if necessary.

Article 28b
Obligations of the provider of a foundation model

1. A provider of a foundation model shall, prior to making it available on the market or putting it into service, ensure that it is compliant with the requirements set out in this Article, regardless of whether it is provided as a standalone model or embedded in an AI system or a product, or provided under free and open source licences, as a service, as well as other distribution channels.

2. For the purpose of paragraph 1, the provider of a foundation model shall:

(a) demonstrate through appropriate design, testing and analysis that the identification, the reduction and mitigation of reasonably foreseeable risks to health, safety, fundamental rights, the environment and democracy and the rule of law prior and throughout development with appropriate methods such as with the involvement of independent experts, as well as the documentation of remaining non-mitigable risks after development;

(b) process and incorporate only datasets that are subject to appropriate data governance measures for foundation models, in particular measures to examine the suitability of the data sources and possible biases and appropriate mitigation;

c) design and develop the foundation model in order to achieve throughout its lifecycle appropriate levels of performance, predictability, interpretability,

corrigibility, safety and cybersecurity assessed through appropriate methods such as model evaluation with the involvement of independent experts, documented analysis, and extensive testing during conceptualisation, design, and development;

(d) design and develop the foundation model, making use of applicable standards to reduce energy use, resource use and waste, as well as to increase energy efficiency, and the overall efficiency of the system. This shall be without prejudice to relevant existing Union and national law and this obligation shall not apply before the standards referred to in Article 40 are published. They shall be designed with capabilities enabling the measurement and logging of the consumption of energy and resources, and, where technically feasible, other environmental impact the deployment and use of the systems may have over their entire lifecycle;

(e) draw up extensive technical documentation and intelligible instructions for use in order to enable the downstream providers to comply with their obligations pursuant to Articles 16 and 28.1.;

(f) establish a quality management system to ensure and document compliance with this Article, with the possibility to experiment in fulfilling this requirement,

(g) register that foundation model in the EU database referred to in Article 60, in accordance with the instructions outlined in Annex VIII paragraph C.

When fulfilling those requirements, the generally acknowledged state of the art shall be taken into account, including as reflected in relevant harmonised standards or common specifications, as well as the latest assessment and measurement methods, reflected notably in benchmarking guidance and capabilities referred to in Article 58a (new).

3. Providers of foundation models shall, for a period ending 10 years after their foundation models have been placed on the market or put into service, keep the technical documentation referred to in paragraph 1(c) at the disposal of the national competent authorities;

4. Providers of foundation models used in AI systems specifically intended to generate, with varying levels of autonomy, content such as complex text, images, audio, or video ("generative AI") and providers who specialise a foundation model into a generative AI system, shall in addition

a) comply with the transparency obligations outlined in Article 52 (1),

b) train, and where applicable, design and develop the foundation model in such a way as to ensure adequate safeguards against the generation of content in breach of Union law in line with the generally-acknowledged state of the art, and without prejudice to fundamental rights, including the freedom of expression,

c) without prejudice to national or Union legislation on copyright, document and make publicly available a sufficiently detailed summary of the use of training data protected under copyright law.

Article 29
*Obligations of **deployers** of high-risk AI systems*

1. ***Deployers*** of high-risk AI systems shall ***take appropriate technical and organisational measures to ensure they*** use such systems in accordance with the instructions of use accompanying the systems, pursuant to paragraphs 2 and 5 ***of this Article***.

1a. To the extent deployers exercise control over the high-risk AI system, they shall

i) implement human oversight according to the requirements laid down in this Regulation

(ii) ensure that the natural persons assigned to ensure human oversight of the high-risk AI systems are competent, properly qualified and trained, and have the necessary resources in order to ensure the effective supervision of the AI system in accordance with Article 14

(iii) ensure that relevant and appropriate robustness and cybersecurity measures are regularly monitored for effectiveness and are regularly adjusted or updated.

2. The obligations in paragraph 1, ***1a, 1b and 1c*** are without prejudice to other ***deployer*** obligations under Union or national law and to the ***deployer's*** discretion in organising its own resources and activities for the purpose of implementing the human oversight measures indicated by the provider.

3. Without prejudice to paragraph 1, ***1a, 1b and 1c,*** to the extent the ***deployer*** exercises control over the input data, that ***deployer*** shall ensure that input data is relevant ***and sufficiently representative*** in view of the intended purpose of the high-risk AI system.

4. ***Deployers*** shall monitor the operation of the high-risk AI system on the basis of the instructions of use ***and when relevant, inform providers in accordance with Article 61.*** When they have reasons to consider that the use in accordance with the instructions of use may result in the AI system presenting a risk within the meaning of Article 65(1) they shall, ***without undue delay,*** inform the provider or distributor ***and relevant national supervisory authorities*** and suspend the use of the system. They shall also ***immediately*** inform ***first*** the provider***, and then the importer*** or distributor ***and relevant national supervisory authorities*** when they have identified any serious incident or any malfunctioning within the meaning of Article 62 and interrupt the use of the AI system. In case the ***deployer*** is not able to reach the provider, Article 62 shall apply mutatis mutandis.

   For ***deployers*** that are credit institutions regulated by Directive 2013/36/EU, the monitoring obligation set out in the first subparagraph shall be deemed to be fulfilled by complying with the rules on internal governance arrangements, processes and mechanisms pursuant to Article 74 of that Directive.

5. ***Deployers*** of high-risk AI systems shall keep the logs automatically generated by that high-risk AI system, to the extent ***that*** such logs are under their control ***and are***

required for ensuring and demonstrating compliance with this Regulation, for ex-post audits of any reasonably foreseeable malfunction, incidents or misuses of the system, or for ensuring and monitoring for the proper functioning of the system throughout its lifecycle. Without prejudice to applicable Union or national law, the logs shall be kept for a period ***of at least 6 months. The retention period shall be in accordance with industry standards and*** appropriate ***to*** the intended purpose of the high-risk AI system ~~and applicable legal obligations under Union or national law.~~

Deployers that are credit institutions regulated by Directive 2013/36/EU shall maintain the logs as part of the documentation concerning internal governance arrangements, processes and mechanisms pursuant to Article 74 of that Directive.

5a. Prior to putting into service or use a high-risk AI system at the workplace, deployers shall consult workers representatives with a view to reaching an agreement and inform the affected employees that they will be subject to the system.

5b. Deployers of high-risk AI systems that are public authorities or Union institutions, bodies, offices and agencies or undertakings referred to in Article 51(1a)(b) shall comply with the registration obligations referred to in Article 51.

6. ***Where applicable, deployers*** of high-risk AI systems shall use the information provided under Article 13 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***, a summary of which shall be published, having regard to the specific use and the specific context in which the AI system is intended to operate. Deployers may revert in part to those data protection impact assessments for fulfilling some of the obligations set out in this article, insofar as the data protection impact assesment fulfill those obligations.***

6a. Without prejudice to Article 52, deployers of high-risk AI systems referred to in Annex III, which make decisions or assist in making decisions related to natural persons, shall inform the natural persons that they are subject to the use of the high-risk AI system. This information shall include the intended purpose and the type of decisions it makes. The deployer shall also inform the natural person about its right to an explanation referred to in Article 68c.

6c. Deployers shall cooperate with the relevant national competent authorities on any action those authorities take in relation with the high-risk system in order to implement this Regulation

Article 29a
Fundamental rights impact assessment for high-risk AI systems

1. Prior to putting a high-risk AI system as defined in Article 6(2) into use, with the exception of AI systems intended to be used in area 2 of Annex III, deployers shall conduct an assessment of the systems' impact in the specific context of use. This assessment shall include, at a minimum, the following elements:

(a) a clear outline of the intended purpose for which the system will be used;

(b) a clear outline of the intended geographic and temporal scope of the system's use;

(c) categories of natural persons and groups likely to be affected by the use of the system;

(d) verification that the use of the system is compliant with relevant Union and national law on fundamental rights;

(e) the reasonably foreseeable impact on fundamental rights of putting the high-risk AI system into use;

(f) specific risks of harm likely to impact marginalised persons or vulnerable groups;

(g) the reasonably foreseeable adverse impact of the use of the system on the environment;

(h) a detailed plan as to how the harms and the negative impact on fundamental rights identified will be mitigated.

(j) the governance system the deployer will put in place, including human oversight, complaint-handling and redress.

2. If a detailed plan to mitigate the risks outlined in the course of the assessment outlined in paragraph 1 cannot be identified, the deployer shall refrain from putting the high-risk AI system into use and inform the provider and the National supervisory authority without undue delay. National supervisory authorities, pursuant to Articles 65 and 67, shall take this information into account when investigating systems which present a risk at national level.

3. The obligation outlined under paragraph 1 applies for the first use of the high-risk AI system. The deployer may, in similar cases, draw back on previously conducted fundamental rights impact assessment or existing assessment carried out by providers. If, during the use of the high-risk AI system, the deployer considers that the criteria listed in paragraph 1 are not longer met, it shall conduct a new fundamental rights impact assessment.

4. In the course of the impact assessment, the deployer, with the exception of SMEs, shall shall notify national supervisory authority and relevant stakeholders and shall, to best extent possible, involve representatives of the persons or groups of persons that are likely to be affected by the high-risk AI system, as identified in paragraph 1, including but not limited to: equality bodies, consumer protection agencies, social partners and data protection agencies, with a view to receiving input into the impact assessment. The deployer must allow a period of six weeks for bodies to respond. SMEs may voluntarily apply the provisions laid down in this paragraph.

In the case referred to in Article 47(1), public authorities may be exempted from this obligations.

5. The deployer that is a public authority or an undertaking referred to in Article 51(1a)(b) shall publish a summary of the results of the impact assessment as part of the registration of use pursuant to their obligation under Article 51(2).

6. Where the deployer is already required to carry out a data protection impact assessment under Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive

(EU) 2016/680, the fundamental rights impact assessment referred to in paragraph 1 shall be conducted in conjunction with the data protection impact assessment. The data protection impact assessment shall be published as an addendum.

Articles 53 to 54a and recitals 71 to 72b	**CA 4**

(71) Artificial intelligence is a rapidly developing family of technologies that requires regulatory oversight and a safe ***and controlled*** space for experimentation, while ensuring responsible innovation and integration of appropriate safeguards and risk mitigation measures. To ensure a legal framework that ***promotes innovation, is*** future-proof, and resilient to disruption, Member States should establish ***at least one*** artificial intelligence regulatory ***sandbox*** 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. ***It is indeed desirable for the establishment of regulatory sandboxes, which establishment is currently left at the discretion of Member States, as a next step to be made mandatory with established criteria. That mandatory sandbox could also be established jointly with one or several other Member States, as long as that sandbox would cover the respective national level of the involved Member States. Additional sandboxes may also be established at different levels, including cross Member States, in order to facilitate cross-border cooperation and synergies. With the exception of the mandatory sandbox at national level, Member States should also be able to establish virtual or hybrid sandboxes. All regulatory sandboxes should be able to accommodate both physical and virtual products. Establishing authorities should also ensure that the regulatory sandboxes have the adequate financial and human resources for their functioning.***

(72) The objectives of the regulatory sandboxes should be: ***for the establishing authorities to increase their understanding of technical developments, improve supervisory methods and provide guidance to AI systems developers and providers to achieve regulatory compliance with this Regulation or where relevant, other applicable Union and Member States legislation, as well as with the Charter of Fundamental Rights; for the prospective providers to allow and facilitate the*** testing ***and*** development ***of innovative solutions related to AI systems in the*** pre-marketing phase to enhance legal certainty~~,~~ ***to allow for more regulatory learning by establishing authorities in a controlled environment to develop better guidance and to identify possible future improvements of the legal framework through the ordinary legislative procedure. Any significant risks identified during the development and testing of such AI systems should result in immediate mitigation and, failing that, in the suspension of the development and testing process until such mitigation takes place.*** To ensure uniform implementation across the Union and economies of scale, it is appropriate to establish common rules for the regulatory sandboxes' implementation and a framework for cooperation between the relevant authorities involved in the supervision of the sandboxes. ***Member States*** should ensure ***that regulatory sandboxes are widely available throughout the Union, while the participation should remain voluntary. It is especially important to ensure that SMEs and startups can easily access these sandboxes, are actively involved and participate*** in the development and ***testing of innovative AI systems, in order to be able to contribute with their knowhow and experience.***

(72a) This Regulation should provide the legal basis for the use of personal data collected for other purposes for developing certain AI systems in the public interest within the AI regulatory sandbox only under specified conditions in line with Article 6(4) of

Regulation (EU) 2016/679, and Article 6 of Regulation (EU) 2018/1725, and without prejudice to Article 4(2) of Directive (EU) 2016/680. Prospective providers in the sandbox should ensure appropriate safeguards and cooperate with the competent authorities, including by following their guidance and acting expeditiously and in good faith to mitigate any high-risks to safety, health and the environment and fundamental rights that may arise during the development and experimentation in the sandbox. The conduct of the prospective providers in the sandbox should be taken into account when competent authorities decide over the temporary or permanent suspension of their participation in the sandbox whether to impose an administrative fine under Article 83(2) of Regulation 2016/679 and Article 57 of Directive 2016/680.

(72b) To ensure that Artificial Intelligence leads to socially and environmentally beneficial outcomes, Member States should support and promote research and development of AI in support of socially and environmentally beneficial outcomes by allocating sufficient resources, including public and Union funding, and giving priority access to regulatory sandboxes to projects led by civil society. Such projects should be based on the principle of interdisciplinary cooperation between AI developers, experts on inequality and non-discrimination, accessibility, consumer, environmental, and digital rights, as well as academics.

TITLE V

MEASURES IN SUPPORT OF INNOVATION

Article 53
AI regulatory sandboxes

1. ***Member States shall establish at least one*** AI regulatory sandbox ***at national level, which shall be operational at the latest on the day of the entry into application of this Regulation. This sandbox can also be established jointly with one or several other Member States.***

1a. Additional AI regulatory sandboxes at regional or local levels or jointly with other Member States may also be established.

1b. The Commission and the European Data Protection Supervisor, on their own, jointly or in collaboration with one or more Member States may also establish AI regulatory sandboxes at Union level.

1c. Establishing authorities shall ***allocate sufficient resources to comply with this Article effectively and in a timely manner.***

1d. AI regulatory sandboxes shall, ***in accordance with criteria set out in Article 53a,*** provide ***for*** a controlled environment ***that fosters innovation and facilitates*** the development, testing and validation of innovative AI systems for a limited time before their placement on the market or putting into service ***pursuant to a specific plan agreed between the prospective providers and the establishing authority.***

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

a) for the competent authorities to provide guidance to AI systems prospective providers to achieve regulatory compliance with this Regulation or where relevant other applicable Union and Member States legislation
b) for the prospective providers to allow and facilitate the testing and development of innovative solutions related to AI systems
c) regulatory learning in a controlled environment

1e. Establishing authorities shall provide guidance and supervision within the sandbox with a view to ***identify risks, in particular to fundamental rights, democracy and rule of law, health and safety and the environment, test and demonstrate mitigation measures for identified risks, and their effectiveness and*** ensure compliance with the requirements of this Regulation and, where relevant, other Union and Member States legislation.

1f. Establishing authorities shall provide sandbox prospective providers who develop high-risk AI systems with guidance and supervision on how to fulfil the requirements set out in this Regulation, so that the AI systems may exit the sandbox being in presumption of conformity with the specific requirements of this Regulation that were assessed within the sandbox. Insofar as the AI system complies with the requirements when exiting the sandbox, it shall be presumed to be in conformity with this regulation. In this regard, the exit reports created by the establishing authority shall be taken into account by market surveillance authorities or notified bodies, as applicable, in the context of conformity assessment procedures or market surveillance checks.

2. ***Establishing authorities*** shall ensure that, to the extent the innovative AI systems involve the processing of personal data or otherwise fall under the supervisory remit of other national authorities or competent authorities providing or supporting access to ***personal*** data, the national data protection authorities, ***or in cases referred to in paragraph 1b the EDPS***, and those other national authorities are associated to the operation of the AI regulatory sandbox ***and involved in the supervision of those aspects to the full extent of their respective tasks and powers***.

3. The AI regulatory sandboxes shall not affect the supervisory and corrective powers of the competent authorities, ***including at regional or local level***. Any significant risks to fundamental rights, ***democracy and rule of law, health and safety or the environment*** identified during the development and testing of such ***AI*** systems shall result in immediate ***and adequate*** mitigation. ***Competent authorities shall have the power to temporarily or permanently suspend the testing process, or participation in the sandbox if no effective mitigation is possible and inform the AI office of such decision.***

4. ***Prospective providers*** in the AI regulatory sandbox shall remain liable under applicable Union and Member States liability legislation for any harm inflicted on third parties as a result ***of*** the experimentation taking place in the sandbox. ***However, provided that the prospective provider(s) respect the specific plan referred to in paragraph 1c and the terms and conditions for their participation and follow in good faith the guidance given by the establishing authorities, no administrative fines*** shall ***be imposed by the authorities for infringements of this Regulation.***

5. ***Establishing authorities*** shall coordinate their activities and cooperate within the framework of the ***AI office.***

5a. Establishing authorities shall inform the AI Office of the establishment of a sandbox and may ask for support and guidance. A list of planned and existing sandboxes shall be made publicly available by the AI office and kept up to date in order to encourage more interaction in the regulatory sandboxes and transnational cooperation.

5b. Establishing authorities shall submit to the AI office and, unless the Commission is the sole establishing authority, to the Commission, annual reports, starting one year after the establishment of the sandbox and then every year until its termination and a final report. Those reports shall provide information on the progress and results–of the implementation of those sandboxes, including best practices, incidents, lessons learnt and recommendations on their setup and, where relevant, on the application and possible revision of this Regulation and other Union legislation supervised within the sandbox Those annual reports or abstracts thereof shall be made available to the public, online.

6. The ***Commission shall develop a single and dedicated interface containing all relevant information related to sandboxes, together with a single contact point at EU level to interact with the*** regulatory sandboxes ***and to allow stakeholders to raise enquiries with competent authorities, and to seek non-binding guidance on the conformity of innovative products, services, business models embedding AI technologies. The Commission*** shall ***proactively coordinate with national, regional and also local authorities, where relevant.***

6a. For the purpose of paragraph 1 and 1a, the Commission shall play a complementary role, enabling Member States to build on their expertise and, on the other hand, assisting and providing technical understanding and resources to those Member States that seek guidance on the set-up and running of these regulatory sandboxes.

Article 53a
Modalities and functioning of AI regulatory sandboxes

1. In order to avoid fragmentation across the Union, the Commission, in consultation with the AI office, shall adopt a delegated act detailing the modalities for the establishment, development, implementation functioning and supervision of the AI regulatory sandboxes, including the eligibility criteria and the procedure for the application, selection, participation and exiting from the sandbox, and the rights and obligations of the participants, based on the provisions set out in this Article

2. The Commission is empowered to adopt delegated acts in accordance with the procedure referred to in Article 73 no later than 12 months following the entry into force of this Regulation and shall ensure that:

a) regulatory sandboxes are open to any applying prospective provider of an AI system who fulfils eligibility and selection criteria. The criteria for accessing to the regulatory sandbox shall be transparent and fair. Establishing authorities shall inform applicants of their decision within 3 months of the application;

b) regulatory sandboxes allow broad and equal access and keep up with demand for participation;

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

d) regulatory sandboxes facilitate the involvement of other relevant actors within the AI ecosystem, such as notified bodies and standardisation organisations (SMEs, start-ups, enterprises, innovators, testing and experimentation facilities, research and experimentation labs and digital innovation hubs, centers of excellence, individual researchers, in order to allow and facilitate cooperation with the public and private sector;

e) they allow prospective providers to fulfil, in a controlled environment, the conformity assessment obligations of this Regulation or the voluntary application of the codes of conduct referred to in Article 69;

f) procedures, processes and administrative requirements for application, selection, participation and exiting the sandbox are simple, easily intelligible, clearly communicated in order to facilitate the participation of SMEs and start-ups with limited legal and administrative capacities and are streamlined across the Union, in order to avoid fragmentation and that participation in a regulatory sandbox established by a Member State, by the Commission, or by the EDPS is mutually and uniformly recognised and carries the same legal effects across the Union;

g) participation in the AI regulatory sandbox is limited to a period that is appropriate to the complexity and scale of the project;

h) the sandboxes shall facilitate the development of tools and infrastructure for testing, benchmarking, assessing and explaining dimensions of AI systems relevant to sandboxes, such as accuracy, robustness and cybersecurity as well as minimisation of risks to fundamental rights, environment and the society at large.

3. Prospective providers in the sandboxes, in particular SMEs and start-ups, shall be facilitated access to pre-deployment services such as guidance on the implementation of this Regulation, to other value-adding services such as help with standardisation documents and certification and consultation, and to other Digital Single Market initiatives such as Testing & Experimentation Facilities, Digital Hubs, Centres of Excellence, and EU benchmarking capabilities.

Article 54
Further processing of ~~personal~~ data for developing certain AI systems in the public interest in the AI regulatory sandbox

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

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

   ~~(i) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding~~

~~against and the prevention of threats to public security, under the control and responsibility of the competent authorities. The processing shall be based on Member State or Union law;~~

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

(iii) a high level of protection and improvement of the quality of the environment, ***protection of biodiversity, pollution as well as climate change mitigation and adaptation;***

(iiia) safety and resilience of transport systems, critical infrastructure and networks.

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

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

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

(e) any personal data processed are not be transmitted, transferred or otherwise accessed by other parties;

(f) any processing of personal data in the context of the sandbox do not lead to measures or decisions affecting the data subjects ***nor affect the application of their rights laid down in Union law on the protection of personal data***;

(g) any personal data processed in the context of the sandbox are ***protected by means of appropriate technical and organisational measures and*** deleted once the participation in the sandbox has terminated or the personal data has reached the end of its retention period;

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

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

(j) a short summary of the AI ***system*** developed in the sandbox, its objectives***,*** ***hypotheses,*** and expected results***,*** published on the website of the competent authorities.

2. Paragraph 1 is without prejudice to Union or Member States legislation excluding processing for other purposes than those explicitly mentioned in that legislation.

Article 54 a

Promotion of AI research and development in support of socially and environmentally beneficial outcomes

1. Member States shall promote research and development of AI solutions which support socially and environmentally beneficial outcomes, including but not limited to development of AI-based solutions to increase accessibility for persons with disabilities, tackle socio-economic inequalities, and meet sustainability and environmental targets, by:

(a) providing relevant projects with priority access to the AI regulatory sandboxes to the extent that they fulfil the eligibility conditions;

(b) earmarking public funding, including from relevant EU funds, for AI research and development in support of socially and environmentally beneficial outcomes;

(c) organising specific awareness raising activities about the application of this Regulation, the availability of and application procedures for dedicated funding, tailored to the needs of those projects;

(d) where appropriate, establishing accessible dedicated channels, including within the sandboxes, for communication with projects to provide guidance and respond to queries about the implementation of this Regulation.

2. Member States shall support civil society and social stakeholders to lead or participate in such projects.

Articles 8 to 12, Annex IV and recitals 42-46b	**CA 5**

(42) To mitigate the risks from high-risk AI systems placed or otherwise put into service on the Union market for ***deployers*** and affected persons, certain mandatory requirements should apply, taking into account the intended purpose, ***the reasonably foreseeable misuse*** of the system and according to the risk management system to be established by the provider. ***These requirements should be objective-driven, fit for purpose, reasonable and effective, without adding undue regulatory burdens or costs on operators.***

(43) Requirements should apply to high-risk AI systems as regards the quality ***and relevance*** of data sets used, technical documentation and record-keeping, transparency and the provision of information to ***deployers***, human oversight, and robustness, accuracy and cybersecurity. Those requirements are necessary to effectively mitigate the risks for health, safety and fundamental rights, as ***well as the environment, democracy and rule of law, as*** applicable in the light of the intended purpose ***or reasonably foreseeable misuse*** of the system, and no other less trade restrictive measures are reasonably available, thus avoiding unjustified restrictions to trade.

(44) ***Access to high*** data quality ***plays a vital role in providing structure and in ensuring*** the performance of many AI systems, especially when techniques involving the training of models are used, with a view to ensure that the high-risk AI system performs as intended and safely and it does not become ***a*** source of discrimination prohibited by Union law. High quality training, validation and testing data sets require the implementation of appropriate data governance and management practices. Training, ***and where applicable,*** validation and testing data sets***, including the labels,*** should be sufficiently relevant, representative***, appropriately vetted for*** errorsand ***as*** complete ***as possible*** in view of the intended purpose of the system. They should also have the appropriate statistical properties, including as regards the persons or groups of persons ***in relation to whom*** the high-risk AI system is intended to be used, ***with specific attention to the mitigation of possible biases in the datasets, that might lead to risks to fundamental rights or discriminatory outcomes for the persons affected by the high-risk AI system***. ***Biases can for example be inherent in underlying datasets, especially when historical data is being used, introduced by the developers of the algorithms, or generated when the systems are implemented in real world settings. Results provided by AI systems are influenced by such inherent biases that are inclined to gradually increase and thereby perpetuate and amplify existing discrimination, in particular for persons belonging to certain vulnerable or ethnic groups, or racialised communities.*** In particular, training, validation and testing data sets should take into account, to the extent required in the light of their intended purpose, the features, characteristics or elements that are particular to the specific geographical, ***contextal,*** behavioural or functional setting or context within which the AI system is intended to be used. In order to protect the right of others from the discrimination that might result from the bias in AI systems, the providers should, ***exceptionally and following the application of all applicable conditions laid down under this Regulation and the Regulation (EU) 2016/679, Directive 2016/680 and Regulation (EU) 2018/1725,*** be able to process also special categories of personal data,

as a matter of substantial public interest, in order to ensure the ***negative*** bias detection and correction in relation to high-risk AI systems. ***Negative bias should be understood as bias that create direct or indirect discriminatory effect against a natural person The requirements related to data governance can be complied with by having recourse to third-parties that offer certified compliance services including verification of data governance, data set integrity, and data training, validation and testing practices.***

(45) For the development ***and assessment*** of high-risk AI systems, certain actors, such as providers, notified bodies and other relevant entities, such as digital innovation hubs, testing experimentation facilities and researchers, should be able to access and use high quality datasets within their respective fields of activities which are related to this Regulation. European common data spaces established by the Commission and the facilitation of data sharing between businesses and with government in the public interest will be instrumental to provide trustful, accountable and non-discriminatory access to high quality data for the training, validation and testing of AI systems. For example, in health, the European health data space will facilitate non-discriminatory access to health data and the training of artificial intelligence algorithms on those datasets, in a privacy-preserving, secure, timely, transparent and trustworthy manner, and with an appropriate institutional governance. Relevant competent authorities, including sectoral ones, providing or supporting the access to data may also support the provision of high-quality data for the training, validation and testing of AI systems.

(45a) The right to privacy and to protection of personal data must be guaranteed throughout the entire lifecycle of the AI system. In this regard, the principles of data minimisation and data protection by design and by default, as set out in Union data protection law, are essential when the processing of data involves significant risks to the fundamental rights of individuals. Providers and users of AI systems should implement state-of-the-art technical and organisational measures in order to protect those rights. Such measures should include not only anonymisation and encryption, but also the use of increasingly available technology that permits algorithms to be brought to the data and allows valuable insights to be derived without the transmission between parties or unnecessary copying of the raw or structured data themselves

(46) Having ***comprehensible*** information on how high-risk AI systems have been developed and how they perform throughout their ***lifetime*** is essential to verify compliance with the requirements under this Regulation. This requires keeping records and the availability of a technical documentation, containing information which is necessary to assess the compliance of the AI system with the relevant requirements. Such information should include the general characteristics, capabilities and limitations of the system, algorithms, data, training, testing and validation processes used as well as documentation on the relevant risk management system. The technical documentation should be kept up to date ***appropriately throughout the lifecycle of the AI system***. ***AI systems can have a large important environmental impact and high energy consumption during their lifecyle. In order to better apprehend the impact of AI systems on the environment, the technical documentation drafted by providers should include information on the energy consumption of the AI system, including the consumption during development and expected consumption during use. Such information should take into account the relevant Union and national legislation. This reported information should be comprehensible, comparable and verifiable and***

to that end, the Commission should develop guidelines on a harmonised metholodogy for calculation and reporting of this information. To ensure that a single documentation is possible, terms and definitions related to the required documentation and any required documentation in the relevant Union legislation should be aligned as much as possible.

(46a) AI systems should take into account state-of-the art methods and relevant applicable standards to reduce the energy use, resource use and waste, as well as to increase their energy efficiency and the overall efficiency of the system. The environmental aspects of AI systems that are significant for the purposes of this Regulation are the energy consumption of the AI system in the development, training and deployment phase as well as the recording and reporting and storing of this data. The design of AI systems should enable the measurement and logging of the consumption of energy and resources at each stage of development, training and deployment. The monitoring and reporting of the emissions of AI systems must be robust, transparent, consistent and accurate. In order to ensure the uniform application of this Regulation and stable legal ecosystem for providers and deployers in the Single Market, the Commission should develop a common specification for the methodology to fulfil the reporting and documentation requirement on the consumption of energy and resources during development, training and deployment. Such common specifications on measurement methodology can develop a baseline upon which the Commission can better decide if future regulatory interventions are needed, upon conducting an impact assessment that takes into account existing legislation;

(46b) In order to achieve the objectives of this Regulation, and contribute to the EU's environmental objectives while ensuring the smooth functioning of the internal market and it may be necessary to establish recommendations and guidelines and, eventually, targets for sustainability. For that purpose the Commission is entitled to develop a methodology to contribute towards having Key Performance Indicators (KPIs) and a reference for the Sustainable Development Goals (SDGs). The goal should be in the first instance to enable fair comparison between AI implementation choices providing incentives to promote using more efficient AI technologies addressing energy and resource concerns. To meet this objective this Regulation should provide the means to establish a baseline collection of data reported on the emissions from development and training and for deployment.

REQUIREMENTS FOR HIGH-RISK AI SYSTEMS

Article 8
Compliance with the requirements

1. High-risk AI systems shall comply with the requirements established in this Chapter.

1a. In complying with the requirement established in this Chapter, due account shall be taken of guidelines developed as referred to in Article 82b, the generally acknowledged state of the art, including as reflected in the relevant harmonised standards and common specifications as referred to in articles 40 and 41 or those already set out in union harmonisation legislation.

2. The intended purpose of the high-risk AI system, ***the reasonably foreseeable misuses*** and the risk management system referred to in Article 9 shall be taken into account when ensuring compliance with those requirements.

2a. As long as the requirements of Title III, Chapters 2 and 3 or Title VIII, Chapters 1, 2 and 3 for high-risk AI systems are addressed by Union Harmonisation Legislation listed in Annex II, Section A, the requirements or obligations of those Chapters of this Regulation shall be deemed to be fulfilled, as long as they include the AI component. Requirements of Chapters 2 and 3 of Title III or Title VIII, Chapters 1, 2 and 3 for high-risk AI systems not addressed by Union Harmonisation Legislation listed in Annex II Section A, shall be incorporated into that Union Harmonisation Legislation, where applicable. The relevant conformity assessment shall be carried out as part of the procedures laid out under Union Harmonisation Legislation listed in Annex II, Section A.

Article 9
Risk management system

1. A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems, ***throughout the entire lifecycle of the AI system. The risk management system can be integrated into, or a part of, already existing risk management procedures relating to the relevant Union sectoral legislation insofar as it fulfils the requirements of this article.***

2. The risk management system shall consist of a continuous iterative process run throughout the entire ***lifecycle*** of a high-risk AI system, requiring regular ***review and*** updating ***of the risk management process, to ensure its continuing effectiveness, and documentation of any significant decisions and actions taken subject to this Article***. It shall comprise the following steps:

(a) identification***, estimation and evaluation*** of the known and ***the reasonably*** foreseeable risks ***that the*** high-risk AI system ***can pose to the health or safety of natural persons, their fundamental rights including equal access and opportunities, democracy and rule of law or the environement when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse.***

~~(b) estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse;~~

(c) evaluation of ***emerging significant*** risks ***as described in paragraph 2(a) and identified*** based on the analysis of data gathered from the post-market monitoring system referred to in Article 61;

(d) adoption of ***appropriate and targeted*** risk management measures ***designed to address the risks identified pursuant to letters a and b of***

this paragraph in accordance with the provisions of the following paragraphs.

3. The risk management measures referred to in paragraph 2, point (c) shall give due consideration to the effects and possible interactions resulting from the combined application of the requirements set out in this Chapter 2, ***with a view to mitigate risks effectively while ensuring an appropriate and proportionate implementation of the requirements.*** ~~They shall take into account the generally acknowledged state of the art, including as reflected in relevant harmonised standards or common specifications.~~

4. The risk management measures referred to in paragraph 2, point (c) shall be such that ***relevant*** residual risk associated with each hazard as well as the overall residual risk of the high-risk AI systems is ***reasonably*** judged ***to be*** acceptable, provided that the high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse. Those residual risks ***and the reasoned judgements made*** shall be communicated to the ***deployer***.
In identifying the most appropriate risk management measures, the following shall be ***ensured***:

   (a) elimination or reduction of ***identified*** risks as far as ***technically feasible*** through adequate design and development ***of the high-risk AI system, involving when relevant, experts and external stakeholders***;
   (b) where appropriate, implementation of adequate mitigation and control measures ***addressing significant*** risks that cannot be eliminated;
   (c) provision of ***the required*** information pursuant to Article 13, ~~in particular as regards the risks referred to in paragraph 2, point (b) of this Article~~ and, where appropriate, training to ***deployers***.

In eliminating or reducing risks related to the use of the high-risk AI system, ***providers shall take into*** due consideration ~~shall be given to~~ the technical knowledge, experience, education, ***and*** training ~~to be expected by~~ the ***deployer may need, including in relation to*** the ***presumable context of use*** ~~in which the system is intended to be used.~~

5. High-risk AI systems shall be tested for the purposes of identifying the most appropriate ***and targeted*** risk management measures ***and weighing any such measures against the potential benefits and intended goals of the system***. Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and they are in compliance with the requirements set out in this Chapter.

6. Testing procedures shall be suitable to achieve the intended purpose of the AI system ~~and do not need to go beyond what is necessary to achieve that purpose.~~

7. The testing of the high-risk AI systems shall be performed ~~as appropriate, at any point in time throughout the development process, and, in any event,~~ prior to the placing on the market or the putting into service. Testing shall be made against ***prior*** defined metrics, and probabilistic thresholds that are appropriate to the intended purpose ***or reasonably foreseeable misuse*** of the high-risk AI system.

8. When implementing the risk management system described in paragraphs 1 to 7, ***providers shall give*** specific consideration ~~shall be given~~ to whether the high-risk AI system is likely to ***adversely impact vulnerable groups of people or children.***

9. For ***providers and AI systems already covered by Union law that require them to establish a specific risk management, including*** credit institutions regulated by Directive 2013/36/EU, the aspects described in paragraphs 1 to 8 shall be part of ***or combined with*** the risk management procedures established by ***those acts of Union law.*** ~~.~~

Article 10
Data and data governance

1. High-risk AI systems which make use of techniques involving the training of models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5 ***as far as this is technically feasible according to the specific market segment or scope of application***.

   Techniques that do not require labelled input data, such as unsupervised learning and reinforcement learning shall be developed on the basis of data sets such as for testing and verification that meet the quality criteria referred to in paragraphs 2 to 5.

2. Training, validation and testing data sets shall be subject to ~~–~~data governance ***appropriate for the intended purpose of the AI system.*** Those ***practices*** shall concern in particular,

   (a) the relevant design choices;

   (aa) transparency as regards the original purpose of data collection;

   (b) data collection ***processes***

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

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

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

   (f) examination in view of possible biases ***that are likely to affect the health and safety of persons, negatively impact fundamental rights or lead to discrimination prohibited under Union law***, ***especially where data outputs influence inputs for future operations ('feedback loops') and***

   (fa) appropriate measures to detect, prevent and mitigate possible biases;

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

3. Training ***datasets, and where they are used*** validation and testing datasets, ***including the labels*** shall be relevant, ***sufficiently*** representative, ***appropriately vetted for*** errors and ***be as*** complete ***as possible in view of the intended purpose***. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons ***in relation to whom*** the high-risk AI system is intended to be used. These characteristics of the datasets ***shall*** be met at the level of individual datasets or a combination thereof.

4. ~~Training, validation and testing d~~ ***D***atasets shall take into account, to the extent required by the intended purpose ***or reasonably foreseeable misuses of the AI system*** the characteristics or elements that are particular to the specific geographical, ***contextual,*** behavioural or functional setting within which the high-risk AI system is intended to be used.

5. To the extent that it is strictly necessary for the purposes of ensuring ***negative*** bias detection and correction in relation to the high-risk AI systems, the providers of such systems may ***exceptionally*** process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving. ***In particular, all the following conditions shall apply in order for this processing to occur:***

   (a) the bias detection and correction cannot be effectively fulfilled by processing synthetic or anonymised data;
   (b) the data are pseudonymised;
   (c) the provider takes appropriate technical and organisational measures to ensure that the data processed for the purpose of this paragraph are secured, protected, subject to suitable safeguards and only authorised persons have access to those data with appropriate confidentiality obligations;
   (d) the data processed for the purpose of this paragraph are not to be transmitted, transferred or otherwise accessed by other parties;
   (e) the data processed for the purpose of this paragraph are protected by means of appropriate technical and organisational measures and deleted once the bias has been corrected or the personal data has reached the end of its retention period;
   (f) effective and appropriate measures are in place to ensure availability, security and resilience of processing systems and services against technical or physical incidents;
   (g) effective and appropriate measures are in place to ensure physical security of locations where the data are stored and processed, internal IT and IT security governance and management, certification of processes and products;

   Providers having recourse to this provision shall draw up documentation explaining why the processing of special categories of personal data was necessary to detect and correct biases.

6. Appropriate data governance and management practices shall apply for the development of high-risk AI systems other than those which make use of techniques involving the training of models in order to ensure that those high-risk AI systems comply with paragraph 2.

6a. ***Where the provider cannot comply with the obligations laid down in this Article because it does not have access to the data and the data is held exclusively by the deployer, the deployer may, on the basis of a contract, be made responsible for any infringement of this Article.***

Article 11
Technical documentation

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

   The technical documentation shall be drawn up in such a way to demonstrate that the high-risk AI system complies with the requirements set out in this Chapter and provide national ***supervisory*** authorities and notified bodies with ~~all~~ the necessary information to assess the compliance of the AI system with those requirements. It shall contain, at a minimum, the elements set out in Annex IV ***or, in the case of SMEs and start-ups, any equivalent documentation meeting the same objectives, subject to approval of the competent national authority***.

2. Where a high-risk AI system related to a product, to which the legal acts listed in Annex II, section A apply, is placed on the market or put into service one single technical documentation shall be drawn up containing all the information set out in ***paragraph 1*** as well as the information required under those legal acts.

3. The Commission is empowered to adopt delegated acts in accordance with Article 73 to amend Annex IV where necessary to ensure that, in the light of technical progress, the technical documentation provides all the necessary information to assess the compliance of the system with the requirements set out in this Chapter.

3a. ***Providers that are credit institutions regulated by Directive 2013/36/EU shall maintain the technical documentation as part of the documentation concerning internal governance, arrangements, processes and mechanisms pursuant to Article 74 of that Directive.***

Article 12
Record-keeping

1. High-risk AI systems shall be designed and developed with capabilities enabling the automatic recording of events ('logs') while the high-risk AI systems is operating. Those logging capabilities shall conform to ***the state of the art and*** recognised standards or common specifications.

2. ***In order to*** ensure a level of traceability of the AI system's functioning throughout its ***entire lifetime*** that is appropriate to the intended purpose of the system***, the logging capabilities shall facilitate the monitoring of operations as referred to in Article 29(4) as well as the post market monitoring referred to in Article 61 . In particular, they shall enable the recording of events relevant for the identification of situations that may:***

   (a) result in the AI system presenting a risk within the meaning of Article 65(1); or

   (b) lead to a substantial modification of the AI system;

2a ***High-risk AI systems shall be designed and developed with the logging capabilities enabling the recording of energy consumption, the measurement or calculation of resource use and environmental impact of the high-risk AI system during all phases of the system's lifecycle***

~~3. In particular, logging capabilities shall enable the monitoring of the operation of the high-risk AI system with respect to the occurrence of situations that may result in the~~

~~AI system presenting a risk within the meaning of Article 65(1) or lead to a substantial modification, and facilitate the post-market monitoring referred to in Article 61.~~

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

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

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

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

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

ANNEX IV
TECHNICAL DOCUMENTATION referred to in Article 11(1)

The technical documentation referred to in Article 11(1) shall contain at least the following information, as applicable to the relevant AI system:

1. A general description of the AI system including:

(a) its intended purpose***, the name of the provider*** and the version of the system ***reflecting its relation to previous and, where applicable, more recent, versions in the succession of revisions***;

(aa) the nature of data likely or intended to be processed by the system and, in the case of personal data, the categories of natural persons and groups likely or intended to be affected

(b) how the AI system ***can interact*** or can be used to interact with hardware or software***, including other AI systems, that are*** not part of the AI system itself, where applicable;

(c) the versions of relevant software or firmware and***, where applicable, information for the deployer on*** any requirement related to version update;

(d) the description of ***the various configurations and variants of*** the AI system ***which are intended to be*** placed on the market or put into service;

(e) the description of hardware on which the AI system is intended to run;

(f) where the AI system is a component of products, photographs or illustrations showing external features, marking and internal layout of those products;

(fa) the description of the deployer interface

(g) instructions of use for the ***deployer in accordance with Article 13(2) and (3) as well as 14(4)(e)*** and, where applicable installation instructions;

(ga) a detailed and easily intellegible description of the system's main optimisation goal or goals

(gb) a detailed and easily intellegible description of the system's expected output and expected output quality

(gc) detailed and easily intellegible instructions for interpreting the system's output

(gd) examples of scenarios for which the system should not be used

2. A detailed description of the elements of the AI system and of the process for its development, including:

(a) the methods and steps performed for the development of the AI system, including, where relevant, recourse to pre-trained systems or tools provided by third parties and how these have been used, integrated or modified by the provider;

(b) ***a description of*** the ***architecture,*** design specifications, ***algorithms and the data structures, including a decomposition of its components and interfaces, how they relate to one another and how they provide for the overall processing or*** logic of the AI system; the key design choices including the rationale and assumptions made, also with regard to persons or groups of persons on which the system is intended to be used; the main classification choices; what the system is designed to optimise for and the relevance of the different parameters; the decisions about any possible trade-off made regarding the technical solutions adopted to comply with the requirements set out in Title III, Chapter 2;

~~(c) the description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing; the computational resources used to develop, train, test and validate the AI system;~~

(d) where relevant, the data requirements in terms of datasheets describing the training methodologies and techniques and the training data sets used, including information about the provenance of those data sets, their scope and main characteristics; how the data was obtained and selected; labelling procedures (e.g. for supervised learning), data cleaning methodologies (e.g. outliers detection);

(e) assessment of the human oversight measures needed in accordance with Article 14, including an assessment of the technical measures needed to facilitate the interpretation of the outputs of AI systems by the ***deployers***, in accordance with Articles 13(3)(d);

(f) where applicable, a detailed description of pre-determined changes to the AI system and its performance, together with all the relevant information related to the technical solutions adopted to ensure continuous compliance of the AI system with the relevant requirements set out in Title III, Chapter 2;

(g) the validation and testing procedures used, including information about the validation and testing data used and their main characteristics; metrics used to measure accuracy, robustness, ~~cybersecurity~~ and compliance with other relevant requirements set out in Title III, Chapter 2 as well as potentially discriminatory impacts; test logs and all test reports dated and signed by the responsible persons, including with regard to pre-determined changes as referred to under point (f);

(ga) cybersecurity measures put in place.

3. Detailed information about the monitoring, functioning and control of the AI system, in particular with regard to: its capabilities and limitations in performance, including the degrees of accuracy for specific persons or groups of persons on which the system is intended to be used and the overall expected level of accuracy in relation to its intended purpose ; the foreseeable unintended outcomes and sources of risks to health and safety, fundamental rights and discrimination in view of the intended purpose of the AI system; the human oversight measures needed in accordance with Article 14, including the technical measures put in place to facilitate the interpretation of the outputs of AI systems by the ***deployers***; specifications on input data, as appropriate;

3a. A description of the appropriateness of the performance metrics for the specific AI system

3b. Information about the energy consumption of the AI system during the development phase and the expected energy consumption during use taking into account, where applicable, relevant Union and national legislation;

4. A detailed description of the risk management system in accordance with Article 9;

5. A description of any ***relevant*** change made ***by providers*** to the system through its ***lifecycle***

6. 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; where no such harmonised standards have been applied, a detailed description of the solutions adopted to meet the requirements set out in Title III, Chapter 2, including a list of other relevant standards ***or common specifications*** applied

7. A copy of the EU declaration of conformity;

8. A detailed description of the system in place to evaluate the AI system performance in the post-market phase in accordance with Article 61, including the post-market monitoring plan referred to in Article 61(3).

Articles 1 and 2, citations 5 a and 5 b, recitals 1-5a and 10-13	**CA 6**

CITATIONS

5a. Having regard to the opinion of the European Central Bank

5b. Having regard to the joint opinion of the European Data Protection Board and the European Data Protection Supervisor

(1) The purpose of this Regulation is ***to promote the uptake of human centric and trustworthy artificial intelligence and to ensure a high level of protection of health, safety, fundamental rights, democracy and rule of law and the environment from harmful effects of artificial intelligence systems in the Union while supporting innovation and improving*** the functioning of the internal market. ***This Regulation lays*** down a uniform legal framework in particular for the development, ***the placing on the market, the putting into service and the*** use of artificial intelligence in conformity with Union values ***and*** ensures the free movement of AI-based goods and services cross-border, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation. ***Certain AI systems can also have an impact on democracy and rule of law and the environment. For the purposes of this Regulation, these concerns are specifically addressed in the critical sectors and use cases listed in Annex III Point 8, and in Art 15a and Annex IV point 3b respectively.***

(1a) This Regulation should preserve the values of the Union facilitating the distribution of artificial intelligence benefits across society, protecting individuals, companies, democracy and rule of law and the environment from risks while boosting innovation and employment and making Europe a leader in the field

(2) Artificial intelligence systems (AI systems) can be easily deployed in multiple sectors of the economy and society, including cross border, and circulate throughout the Union. Certain Member States have already explored the adoption of national rules to ensure that artificial intelligence is ***trustworthy and*** safe and is developed and used in compliance with fundamental rights obligations. Differing national rules may lead to fragmentation of the internal market and decrease legal certainty for operators that develop or use AI systems. A consistent and high level of protection throughout the Union should therefore be ensured ***in order to achieve trustworthy AI***, while divergences hampering the free circulation, ***innovation, deployment and uptake*** of AI systems and related products and services within the internal market should be prevented, by laying down uniform obligations for operators and guaranteeing the uniform protection of overriding reasons of public interest and of rights of persons throughout the internal market based on Article 114 of the Treaty on the Functioning of the European Union (TFEU).

(2a) As artificial intelligence often relies on the processing of large volumes of data, and many AI systems and applications on the processing of personal data, it is appropriate to base this Regulation on Article 16 TFEU, which enshrines the right to the

protection of natural persons with regard to the processing of personal data and provides for the adoption of rules on the protection of individuals with regard to the processing of personal data.

(2b) The fundamental right to the protection of personal data is safeguarded in particular by Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive 2016/680. Directive 2002/58/EC additionally protects private life and the confidentiality of communications, including providing conditions for any personal and non-personal data storing in and access from terminal equipment. Those legal acts provide the basis for sustainable and responsible data processing, including where datasets include a mix of personal and nonpersonal data. This Regulation does not seek to affect the application of existing Union law governing the processing of personal data, including the tasks and powers of the independent supervisory authorities competent to monitor compliance with those instruments. This Regulation does not affect the fundamental rights to private life and the protection of personal data as provided for by Union law on data protection and privacy and enshrined in the Charter of Fundamental Rights of the European Union (the 'Charter').

(2c) Artificial intelligence systems in the Union are subject to relevant product safety legislation that provides a framework protecting consumers against dangerous products in general and such legislation should continue to apply. This Regulation is also without prejudice to the rules laid down by other Union legal acts related to consumer protection and product safety, including Regulation (EU) 2017/2394, Regulation (EU) 2019/1020 and Directive 2001/95/EC on general product safety and Directive 2013/11/EU..

(2d) In line with Article 114(2) TFEU, this Regulation complements and should not undermine the rights and interests of employed persons. This Regulation should therefore not affect Community law on social policy and national labour law and practice, that is any legal and contractual provision concerning employment conditions, working conditions, including health and safety at work and the relationship between employers and workers, including information, consultation and participation. This Regulation should not affect the exercise of fundamental rights as recognized in the Member States and at Union level, including the right or freedom to strike or to take other action covered by the specific industrial relations systems in Member States, in accordance with national law and/or practice. Nor should it affect concertation practices, the right to negotiate, to conclude and enforce collective agreement or to take collective action in accordance with national law and/or practice. It should in any case not prevent the Commission from proposing specific legislation on the rights and freedoms of workers affected by AI systems.

(2e) This Regulation should not affect the provisions aimed at improving working conditions in platform work set out in Directive 2021/762/EC.

(2f) This Regulation should help in supporting research and innovation and should not undermine research and development activity and respect freedom of scientific research. It is therefore necessary to exclude from its scope AI systems specifically developed for the sole purpose of scientific research and development and to ensure that the Regulation does not otherwise affect scientific research and development activity on AI systems. Under all circumstances, any research and development

activity should be carried out in accordance with the Charter of fundamental rights, Union law as well as the law of the Member States

(3) Artificial intelligence is a fast evolving family of technologies that ***can and already contributes*** to a wide array of economic, ***environmental*** and societal benefits across the entire spectrum of industries and social activities ***if developed in accordance with relevant general principles in line with the EU Charter of Fundamental Rights and the values on which the Union is founded***. By improving prediction, optimising operations and resource allocation, and personalising digital solutions available for individuals and organisations, the use of artificial intelligence can provide key competitive advantages to companies and support socially and environmentally beneficial outcomes, for example in healthcare, farming, ***food safety,*** education and training, ***media, sports, culture***, infrastructure management, energy, transport and logistics, ***crisis management***, public services, security, justice, resource and energy efficiency, ***environmental monitoring, the conservation and restoration of biodiversity and ecosystems*** and climate change mitigation and adaptation.

(3a) To contribute to reaching the carbon neutrality targets, European companies should seek to utilise all available technological advancements that can assist in realising this goal. Artificial Intelligence is a technology that has the potential of being used to process the ever-growing amount of data created during industrial, environmental, health and other processes. To facilitate investments in AI-based analysis and optimisation tools, this Regulation should provide a predictable and proportionate environment for low-risk industrial solutions.

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

(4a) Given the major impact that artificial intelligence can have on society and the need to build trust, it is vital for artificial intelligence and its regulatory framework to be developed according to Union values enshrined in Article 2 TEU, the fundamental rights and freedoms enshrined in the Treaties, the Charter, and international human rights law. As a pre-requisite, artificial intelligence should be a human-centric technology. It should not substitute human autonomy or assume the loss of individual freedom and should primarily serve the needs of the society and the common good. Safeguards should be provided to ensure the development and use of ethically embedded artificial intelligence that respects Union values and the Charter.

(5) A Union legal framework laying down harmonised rules on artificial intelligence is therefore needed to foster the development, use and uptake of artificial intelligence in the internal market that at the same time meets a high level of protection of public interests, such as health and safety,protection of fundamental rights, ***democracy and rule of law and the environment,*** as recognised and protected by Union law. To achieve that objective, rules regulating the placing on the market, ***the*** putting into service ***and the use*** of certain AI systems should be laid down, thus ensuring the smooth functioning of the internal market and allowing those systems to benefit from the principle of free movement of goods and services. ***These rules should be clear and robust in protecting fundamental rights, supportive of new innovative solutions, and enabling to a European ecosystem of public and private actors creating AI systems in line with EU***

values. By laying down those rules ***as well as measures in support of innovation with a particular focus on SMEs and start-ups***, this Regulation supports the objective of ***promoting the "AI made in Europe, of*** the Union of being a global leader in the development of secure, trustworthy and ethical artificial intelligence, as stated by the European Council[4], and it ensures the protection of ethical principles, as specifically requested by the European Parliament[5].

(5a) Furthermore, in order to foster the development of artificial intelligence systems in line with Union values, the Union needs to address the main gaps and barriers blocking the potential of the digital transformation including the shortage of digitally skilled workers, cybersecurity concerns, lack of investment and access to investment, and existing and potential gaps between large companies, SME's and start-ups. Special attention should be paid to ensuring that the benefits of AI and innovation in new technologies are felt across all regions of the Union and that sufficient investment and resources are provided especially to those regions that may be lagging behind in some digital indicators.

(10) In order to ensure a level playing field and an effective protection of rights and freedoms of individuals across the Union ***and on international level***, the rules established by this Regulation should apply to providers of AI systems in a non-discriminatory manner, irrespective of whether they are established within the Union or in a third country, and to ***deployers*** of AI systems established within the Union. ***In order for the European Union to be true to its fundamental values, AI systems intended to be used for practices that are considered unacceptable by this Regulation, should equally be deemed unacceptable outside the EU because of their particularly harmful effect to fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union. Therefore it is appropriate to prohibit the export of such AI systems to third countries by providers residing in the Union.***

(11) In light of their digital nature, certain AI systems should fall within the scope of this Regulation even when they are neither placed on the market, nor put into service, nor used in the Union. This is the case for example of an operator established in the Union that contracts certain services to an operator established outside the Union in relation to an activity to be performed by an AI system that would qualify as high-risk and whose effects impact natural persons located in the Union. In those circumstances, the AI system used by the operator outside the Union could process data lawfully collected in and transferred from the Union, and provide to the contracting operator in the Union the output of that AI system resulting from that processing, without that AI system being placed on the market, put into service or used in the Union. To prevent the circumvention of this Regulation and to ensure an effective protection of natural persons located in the Union, this Regulation should also apply to providers and ~~users~~ ***deployers*** of AI systems that are established in a third country, to the extent the output produced by those systems is ***intended to be*** used in the Union. Nonetheless, to take into account existing arrangements and special needs for cooperation with foreign partners with whom information and evidence is exchanged, this Regulation should not

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

5 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).

apply to public authorities of a third country and international organisations when acting in the framework of international agreements concluded at national or European level for law enforcement and judicial cooperation with the Union or with its Member States. Such agreements have been concluded bilaterally between Member States and third countries or between the European Union, Europol and other EU agencies and third countries and international organisations. ***This exception should nevertheless be limited to trusted countries and international organisation that share Union values.***

(12) This Regulation should also apply to Union institutions, offices, bodies and agencies when acting as a provider or ***deployer*** of an AI system. AI systems exclusively developed or used for military purposes should be excluded from the scope of this Regulation where that use falls under the exclusive remit of the Common Foreign and Security Policy regulated under Title V of the Treaty on the European Union (TEU). This Regulation should be without prejudice to the provisions regarding the liability of intermediary service providers set out in Directive 2000/31/EC of the European Parliament and of the Council [as amended by the Digital Services Act].

(12a) Software and data that are openly shared and where users can freely access, use, modify and redistribute them or modified versions thereof, can contribute to research and innovation in the market. Research by the European Commission also shows that free and open-source software can contribute between €65 billion to €95 billion to the European Union's GDP and that it can provide significant growth opportunities for the European economy. Users are allowed to run, copy, distribute, study, change and improve software and data, including models by way of free and open-source licences. To foster the development and deployment of AI, especially by SMEs, start-ups, academic research but also by individuals, this Regulation should not apply to such free and open-source AI components except to the extent that they are placed on the market or put into service by a provider as part of a high-risk AI system or of an AI system that falls under Title II or IV of this Regulation.

(12b) Neither the collaborative development of free and open-source AI components nor making them available on open repositories should constitute a placing on the market or putting into service. A commercial activity, within the understanding of making available on the market, might however be characterised by charging a price, with the exception of transactions between micro enterprises, for a free and open-source AI component but also by charging a price for technical support services, by providing a software platform through which the provider monetises other services, or by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software.

(12c) The developers of free and open-source AI components should not be mandated under this Regulation to comply with requirements targeting the AI value chain and, in particular, not towards the provider that has used that free and open-source AI component. Developers of free and open-source AI components should however be encouraged to implement widely adopted documentation practices, such as model and data cards, as a way to accelerate information sharing along the AI value chain, allowing the promotion of trustworthy AI systems in the EU.

(13) In order to ensure a consistent and high level of protection of public interests as regards health, safety and fundamental rights ***as well as democracy and rule of law and the environment***, common normative standards for all high-risk AI systems should be established. Those standards should be consistent with the Charter of fundamental

rights of the European Union (the Charter) ***the European Green Deal (The Green Deal), the Joint Declaration on Digital Rights of the Union (the Declaration) and the Ethics Guidelines for Trustworthy Artificial Intelligence (AI) of the High-Level Expert Group on Artificial Intelligence (AI HLEG),*** and should be non-discriminatory and in line with the Union's international trade commitments.

TITLE I

GENERAL PROVISIONS

Article 1
Subject matter

The purpose of this Regulation is to promote the uptake of human centric and trustworthy artificial intelligence and to ensure a high level of protection of health, safety, fundamental rights, democracy and rule of law, and the environment from harmful effects of artificial intelligence systems in the Union while supporting innovation.

This Regulation lays down:

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

b) prohibitions of certain artificial intelligence practices;

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

d) harmonised transparency rules for ***certain*** AI systems ~~intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content~~

e) rules on market monitoring, ***market*** surveillance***, governance and enforcement***

(ea) measures to support innovation, with a particular focus on SMEs and start ups, including on setting up regulatory sandboxes and targeted measures to reduce the regulatory burden on SMEs and start-ups;

(eb) rules for the establishment and functioning of the European Union artificial intelligence Office.

Article 2
Scope

1. This Regulation applies to:

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

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

(c) providers ***and deployers*** of AI systems ***that have their place of establishment or*** are located in a third country, where ***either Member State law applies by virtue of public international law or*** the output produced by the system is ***intended to be*** used in the Union;

(ca) providers placing on the market or putting into service AI systems referred to in Article 5 outside the Union where the provider or distributor of such systems is located within the Union;

(cb) importers and distributors of AI systems as well as authorised representatives of providers of AI systems, where such importers, distributors or authorised representatives have their establishment or are located in the Union;

(cc) affected persons as defined in Article 3(8a) that are located in the Union and whose health, safety or fundamental rights were adversely impacted by the use of an AI system that was placed on the market or put into service in the Union;

2. For high-risk AI systems that are safety components of products or systems, or which are themselves products or systems ***and that fall*** within the scope of ***harmonisation legislation listed in Annex II - Section B***, only Article 84 of this Regulation shall apply:

~~(a) Regulation (EC) 300/2008;~~

~~(b) Regulation (EU) No 167/2013;~~

~~(c) Regulation (EU) No 168/2013;~~

~~(d) Directive 2014/90/EU;~~

~~(e) Directive (EU) 2016/797;~~

~~(f) Regulation (EU) 2018/858;~~

~~(g) Regulation (EU) 2018/1139;~~

~~(h) Regulation (EU) 2019/2144.~~

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

4. This Regulation shall not apply to public authorities in a third country nor to international organisations falling within the scope of this Regulation pursuant to paragraph 1, where those authorities or organisations use AI systems in the framework of international ***cooperation or*** agreements for law enforcement and judicial cooperation with the Union or with one or more Member States ***and are subject of a decision of the Commission adopted in accordance with Article 36 of Directive (EU)2016/680 or Article 45 of Regulation 2016/679 (adequacy decision) or are part of an international agreement concluded between the Union and that third country or international organisation pursuant to Article 218 TFUE providing adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals***.

5. This Regulation shall not affect the application of the provisions on the liability of intermediary service providers set out in Chapter II, Section IV of Directive

2000/31/EC of the European Parliament and of the Council[6] [as to be replaced by the corresponding provisions of the Digital Services Act].

5a. Union law on the protection of personal data, privacy and the confidentiality of communications applies to personal data processes in connection with the rights and obligations laid down in this Regulation. This Regulation shall not affect Regulations (EU) 2016/679, (EU) 2018/1725, Directive 2002/58/EC and (EU) 2016/680 without prejudice to arrangements provided for in Article 54 of this Regulation.

5b. This Regulation is without prejudice to the rules laid down by other Union legal acts related to consumer protection and product safety.

5c. This Regulation shall not preclude Member States or the Union from maintaining or introducing laws, regulations or administrative provisions which are more favourable to workers in terms of protecting their rights in respect of the use of AI systems by employers, or to encourage or allow the application of collective agreements which are more favourable to workers.

5d. This Regulation shall not apply to research, testing and development activities regarding an AI system prior to this system being placed on the market or put into service, provided that these activities are conducted respecting fundamental rights and the applicable Union law. The testing in real world conditions shall not be covered by this exemption. The Commission is empowered to may adopt delegated acts in accordance with Article 73 to specify this exemption to prevent its existing and potential abuse. The AI Office shall provide guidance on the governance of research and development pursuant to Article 56, also aiming at coordinating its application by the national supervisory authorities.

5d. ***This Regulation shall not apply to AI components provided under free and open-source licences except to the extent they are placed on the market or put into service by a provider as part of a high-risk AI system or of an AI system that falls under Title II or IV. This exemption shall not apply to foundation models as defined in Art 3.***

---

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

(83) In order to ensure trustful and constructive cooperation of competent authorities on Union and national level, all parties involved in the application of this Regulation should ***aim for transparency and openness while*** respect***ing*** the confidentiality of information and data obtained in carrying out their tasks ***by putting in place technical and organisational measures to protect the security and confidentiality of the information obtained carrying out their activities including for intellectual property rights and public and national security interests. In cases where the activities of the Commission, national competent authorities and notified bodies pursuant to this Regulation results in a breach of intellectual property rights, Member States should provide for adequate measures and remedies to ensure the enforcement of intellectual property rights in application of Directive 2004/48/EC.***

(84) ***Compliance with this Regulation should be enforceable by means of the imposition of fines by the national supervisory authority when carrying out proceedings under the procedure laid down in this Regulation.*** 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. ***In order to strengthen and harmonise administrative penalties for infringement of this Regulation, this Regulation lays down the upper limits for setting the administrative fines for*** certain specific infringements, ***When assessing the amount of the fines, national competent authorities should, in each individual case, take into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and to the provider's size, in particular if the provider is a SME or a start-up.*** The European Data Protection Supervisor should have the power to impose fines on Union institutions, agencies and bodies falling within the scope of this Regulation. ***The penalties and litigation costs under this Regulation should not be subject to contractual clauses or any other arrangements.***

(84a) As the rights and freedoms of natural and legal persons and groups of natural persons can be seriously undermined by AI systems, it is essential that natural and legal persons or groups of natural persons have meaningful access to reporting and redress mechanisms and to be entitled to access proportionate and effective remedies. They should be able to report infringments of this Regulation to their national supervisory authority and have the right to lodge a complaint against the providers or deployers of AI systems. Where applicable, deployers should provide internal complaints mechanisms to be used by natural and legal persons or groups of natural persons. Without prejudice to any other administrative or non-judicial remedy, natural and legal persons and groups of natural persons should also have the right to an effective judicial remedy with regard to a legally binding decision of a national supervisory authority concerning them or, where the national supervisory authority does not handle a complaint, does not inform the complainant of the progress or preliminary outcome of the complaint lodged or does not comply with its obligation to reach a final decision, with regard to the complaint.

(84b) Affected persons should always be informed that they are subject to the use of a high-risk AI system, when deployers use a high-risk AI system to assist in decision-making or make decisions related to natural persons. This information can provide a basis for affected persons to exercise their right to an explanation under this Regulation. When deployers provide an explanation to affected persons under this Regulation, they should take into account the level of expertise and knowledge of the average consumer or individual

(84c) Union legislation on the protection of whistleblowers (Directive (EU) 2019/1937) has full application to academics, designers, developers, project contributors, auditors, product managers, engineers and economic operators acquiring information on breaches of Union law by a provider of AI system or its AI system.

(85) In order to ensure that the regulatory framework can be adapted where necessary, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to amend ~~the techniques and approaches referred to in Annex I to define AI systems~~, the Union harmonisation legislation listed in Annex II, the high-risk AI systems listed in Annex III, the provisions regarding technical documentation listed in Annex IV, the content of the EU declaration of conformity in Annex V, the provisions regarding the conformity assessment procedures in Annex VI and VII and the provisions establishing the high-risk AI systems to which the conformity assessment procedure based on assessment of the quality management system and assessment of the technical documentation should apply. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making. ***These consultations should involve the participation of a balanced selection of stakeholders, including consumer organisations, civil society, associations representing affected persons, businesses representatives from different sectors and sizes, as well as researchers and scientists.*** In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(85a) Given the rapid technological developments and the required technical expertise in conducting the assessment of high-risk AI systems, the Commission should regularly review Article 5, Articles 52 and Annex III, at least every year, while consulting the AI office and the relevant stakeholders

(86) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council.

(87) Since the objective of this Regulation cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 TEU. In accordance with the principle of

proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(87a) As reliable information on the resource and energy use, waste production and other environmental impact of AI systems and related ICT technology, including software, hardware and in particular data centres, is limited, the Commission should introduce of an adequate methodology to measure the environmental impact and effectiveness of this Regulation in light of the Union environmental and climate objectives.

(88) This Regulation should apply from … [*OP – please insert the date established in Art. 85*]. However, the infrastructure related to the governance and the conformity assessment system should be operational before that date, therefore the provisions on notified bodies and governance structure should apply from … [*OP – please insert the date – three months following the entry into force of this Regulation*]. In addition, Member States should lay down and notify to the Commission the rules on penalties, including administrative fines, and ensure that they are properly and effectively implemented by the date of application of this Regulation. Therefore the provisions on penalties should apply from [*OP – please insert the date – twelve months following the entry into force of this Regulation*].

(89) The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42(2) of Regulation (EU) 2018/1725 and delivered an opinion on ***18.6.2021.***

TITLE X - Confidentiality and penalties

Article 70
Confidentiality

1. ***The Commission,*** national competent authorities and notified ***bodies, the AI Office and any other natural or legal person*** involved in the application of this Regulation shall respect the confidentiality of information and data obtained in carrying out their tasks and activities in such a manner as to protect, in particular:

    a. intellectual property rights, and confidential business information or trade secrets of a natural or legal person, ***in accordance with the provisions of Directive 2004/48/EC and Directive 2016/943/EC*** including source code, except the cases referred to in Article 5 of Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure apply.

    b. the effective implementation of this Regulation, in particular for the purpose of inspections, investigations or audits;

    ba. public and national security interests

c. integrity of criminal or administrative proceedings.

1a. The authorities involved in the application of this Regulation pursuant to paragraph 1 shall minimise the quantity of data requested for disclosure to the data that is strictly necessary for the perceived risk and the assessment of that risk and shall delete the data as soon as it is no longer needed for the purpose it was requested for and they shall put in place adequate and effective cybersecurity, technical and organisational measures to protect the security and confidentiality of the information and data obtained in carrying out their tasks and activities

2. Without prejudice to paragraph***s 1 and*** 1***a***, 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 consultation of the originating national competent authority and the ***deployer*** when high-risk AI systems referred to in points 1, 6 and 7 of Annex III are used by law enforcement, immigration or asylum authorities, when such disclosure would jeopardise public ***or*** national security ~~interests .~~

When the law enforcement, immigration or asylum authorities are providers of high-risk AI systems referred to in points 1, 6 and 7 of Annex III, the technical documentation referred to in Annex IV shall remain within the premises of those authorities. Those authorities shall ensure that the market surveillance authorities referred to in Article 63(5) and (6), as applicable, can, upon request, immediately access the documentation or obtain a copy thereof. Only staff of the market surveillance authority holding the appropriate level of security clearance shall be allowed to access that documentation or any copy thereof.

2. Paragraphs 1, ***1a*** 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 parties concerned to provide information under criminal law of the Member States.

3. The Commission and Member States may exchange, where ***strictly*** necessary ***and in accordance with relevant provisions of international and trade agreements*** confidential information with regulatory authorities of third countries with which they have concluded bilateral or multilateral confidentiality arrangements guaranteeing an adequate level of confidentiality.

Article 71
Penalties

1. In compliance with the terms and conditions laid down in this Regulation, Member States shall lay down the rules on penalties, ~~including administrative fines~~, applicable to infringements of this Regulation ***by any operator***, and shall take all measures necessary to ensure that they are properly and effectively implemented ***and aligned with the guidelines issued by the Commission and the AI Office pursuant to Article 82b .*** The penalties provided for shall be effective, proportionate, and dissuasive. They shall take into ~~particular~~ account the interests of ***SMEs*** and start-up***s*** and their economic viability.

2. The Member States shall notify the Commission ***and the Office by [12 months following the date of entry into force of this Regulation]*** of those rules and of those measures and shall notify ***them***~~,~~ without delay, of any subsequent amendment affecting them.

3. ***Non compliance with the prohibition of the artificial intelligence practices referred to in Article 5*** shall be subject to administrative fines of up to ***40*** 000 000 EUR or, if the offender is ***a*** company, up to ***7*** % of its total worldwide annual turnover for the preceding financial year, whichever is higher;

3a. Non-compliance of the AI system with the requirements laid down in Article 10 and 13 shall be subject to administrative fines of up to 20 000 000 EUR or, if the offender is a company, up to 4% of its total worldwide annual turnover for the preceding financial year, whichever is the higher

4. Non-compliance of AI system or foundation model with any requirements or obligations under this Regulation, other than those laid down in Articles 5, ~~and~~ 10 ***and 13***, shall be subject to administrative fines of up to ***10 000 000*** EUR or, if the offender is a company, up to ***2%*** of its total worldwide annual turnover for the preceding financial year, whichever is higher.

5. The supply of incorrect, incomplete or misleading information to notified bodies and national competent authorities in reply to a request shall be subject to administrative fines of up to - ***5*** 000 000 EUR or, if the offender is a company, up to ***1*** % of its total worldwide annual turnover for the preceding financial year, whichever is higher

6. ***Fines may be imposed in addition to or instead of non-monetary measures such as orders or warnings.*** When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and due regard shall be given to the following:

    a. the nature, gravity and duration of the infringement and of its consequences, ***taking into account the purpose of the AI system, as well as, where appropriate, the number of affected persons and the level of damage suffered by them***;

    b. whether administrative fines have been already applied by other ***supervisory*** authorities ***of one or more Member States*** to the same operator for the same infringement.

    c. the size ***and annual turnover*** of the operator committing the infringement

    (ca) any action taken by the operator to mitigate the harm of damage suffered by the affected persons

    (cb) the intentional or negligent character of the infringement

    (cc) the degree of cooperation with the national competent authorities, in order to remedy the infringement and mitigate the possible adverse effects of the infringement

(cd) the degree of responsibility of the operator taking into account the technical and organisational measures implemented by them;

(ce) the manner in which the infringement became known to the national competent authorities, in particular whether, and if so to what extent, the operator notified the infringement;

(cf) adherence to approved codes of conduct or approved certification mechanisms;

(cg) any relevant previous infringements by the operator

(ch) any other aggravating or mitigating factor applicable to the circumstances of the case

7. Each Member State shall lay down rules on ~~whether and to what extent~~ administrative fines ***to*** be imposed on public authorities and bodies established in that Member State

8. Depending on the legal system of the Member States, the rules on administrative fines may be applied in such a manner that the fines are imposed by competent national courts of other bodies as applicable in those Member States. The application of such rules in those Member States shall have an equivalent effect.

8a. ***The penalties referred to in this article as well as the associated litigation costs and indemnification claims may not be the subject of contractual clauses or other form of burden-sharing agreements between providers and distributors, importers,-deployers, or any other third parties;***

8b. National supervisory authorities shall, on an annual basis, report to the AI Office about the fines they have issued during that year, in accordance with this Article;

8c. The exercise by competent authorities of their powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including judicial remedy and due process

Article 72
Administrative fines on Union institutions, agencies and bodies

1. The European Data Protection Supervisor may impose administrative fines on Union institutions, agencies and bodies falling within the scope of this Regulation. When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and due regard shall be given to the following:

    a) the nature, gravity and duration of the infringement and of its consequences;, ***taking into account the purpose of the AI system concerned as well as the number of affected persons and the level of damage suffered by them, and any relevant previous infringement;***

aa) any action taken by the Union institution, agency or body to mitigate the damage suffered by affected persons;

(ab) the degree of responsibility of the Union institution, agency or body, taking into account technical and organisational measures implemented by them;

b) the ***degree of*** cooperation with the European Data Protection Supervisor in order to remedy the infringement and mitigate the possible adverse effects of the infringement, including compliance with any of the measures previously ordered by the European Data Protection Supervisor against the Union institution or agency or body concerned with regard to the same subject matter

(c) any similar previous infringements by the Union institution, agency or body

(ca) the manner in which the infringement became known to the European Data Protection Supervisor, in particular whether, and if so to what extent, the Union institution or body notified the infringement

(cb) the annual budget of the body

2. ***Non compliance with the prohibition of the artificial intelligence practices referred to in Article 5*** shall be subject to administrative fines of up to ***1 500 000*** -EUR**.**

2a. Non-compliance of the AI system with the requirements laid down in Article 10 ***shall be subject to administrative fines of up to 1 000 000 EUR***

3. The non-compliance of the AI system with any requirements or obligations under this Regulation, other than those laid down in Articles 5 and 10, shall be subject to administrative fines of up to ***750 000*** EUR

4. Before taking decisions pursuant to this Article, the European Data Protection Supervisor shall give the Union institution, agency or body which is the subject of the proceedings conducted by the European Data Protection Supervisor the opportunity of being heard on the matter regarding the possible infringement. The European Data Protection Supervisor shall base his or her decisions only on elements and circumstances on which the parties concerned have been able to comment. Complainants, if any, shall be associated closely with the proceedings.

5. The rights of defense of the parties concerned shall be fully respected in the proceedings. They shall be entitled to have access to the European Data Protection Supervisor's file, subject to the legitimate interest of individuals or undertakings in the protection of their personal data or business secrets.

6. Funds collected by imposition of fines in this Article shall ***contribute to*** the general budget of the Union. ***The fines shall not affect the effective operation of the Union institution, body or agency fined.***

6a. The European Data Protection Supervisor shall, on an annual basis, notify the AI Office of the fines it has imposed pursuant to this Article

TITLE XI - delegation of power and committee procedure

Article 73
Exercise of the delegation

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

2. ***The power to adopt delegated acts referred to in*** Article 4, Article 7(1), Article 11(3), Article 43(5) and (6) and Article 48(5) shall be conferred on the Commission for ***a period of five years*** from [***the date of entry*** into force of the Regulation].***The Commission shall draw up a report in respect of the delegation of power not later than 9 months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.***

3. The delegation of power referred to in Article 4, Article 7(1), Article 11(3), Article 43(5) and (6) and Article 48(5) 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.

3a. Before adopting a delegated act, the Commission shall consult with the relevant institutions, the Office, the Advisory Forum and other relevant stakeholders in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making. Once the Commission decides to draft a delegated act, it shall notify the European Parliament of this fact. This notification does not place an obligation on the Commission to adopt the said act.

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

5. Any delegated act adopted pursuant to Article 4, Article 7(1), Article 11(3), Article 43(5) and (6) and Article 48(5) 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 74
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 XII

FINAL PROVISIONS

Article 75
Amendment to Regulation (EC) No 300/2008

In Article 4(3) of Regulation (EC) No 300/2008, the following subparagraph is added:

"When adopting detailed measures related to technical specifications and procedures for approval and use of security equipment concerning Artificial Intelligence systems in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Chapter 2, Title III of that Regulation shall be taken into account."

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …)."

Article 76
Amendment to Regulation (EU) No 167/2013

In Article 17(5) of Regulation (EU) No 167/2013, the following subparagraph is added:

"When adopting delegated acts pursuant to the first subparagraph concerning artificial intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …)."

Article 77
Amendment to Regulation (EU) No 168/2013

In Article 22(5) of Regulation (EU) No 168/2013, the following subparagraph is added:

"When adopting delegated acts pursuant to the first subparagraph concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX on [Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …)."

Article 78
Amendment to Directive 2014/90/EU

In Article 8 of Directive 2014/90/EU, the following paragraph is added:

"4. For Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, when carrying out its activities pursuant to paragraph 1 and when adopting technical specifications and testing standards in accordance with paragraphs 2 and 3, the Commission shall take into account the requirements set out in Title III, Chapter 2 of that Regulation.

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …).".

Article 79
Amendment to Directive (EU) 2016/797

In Article 5 of Directive (EU) 2016/797, the following paragraph is added:

"12. When adopting delegated acts pursuant to paragraph 1 and implementing acts pursuant to paragraph 11 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …).".

Article 80
Amendment to Regulation (EU) 2018/858

In Article 5 of Regulation (EU) 2018/858 the following paragraph is added:

"4. When adopting delegated acts pursuant to paragraph 3 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council *, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …).".

Article 81
Amendment to Regulation (EU) 2018/1139

Regulation (EU) 2018/1139 is amended as follows:

(1) In Article 17, the following paragraph is added:

"3. Without prejudice to paragraph 2, when adopting implementing acts pursuant to paragraph 1 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [*on Artificial Intelligence*] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.

Article 81a

Amendment to Regulation (EU) 2019/1020

Regulation (EU) 2019/1020 is amended as follows:

In Article 14(4), the following paragraph is added:

"(l) The power to implement the powers provided for in this Article remotely, where applicable."

---

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …)."

(2) In Article 19, the following paragraph is added:

"4. When adopting delegated acts pursuant to paragraphs 1 and 2 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence], the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account."

(3) In Article 43, the following paragraph is added:

"4. When adopting implementing acts pursuant to paragraph 1 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence], the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account."

(4) In Article 47, the following paragraph is added:

"3. When adopting delegated acts pursuant to paragraphs 1 and 2 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence], the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account."

(5) In Article 57, the following paragraph is added:

"When adopting those implementing acts concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence], the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account."

(6) In Article 58, the following paragraph is added:

"3. When adopting delegated acts pursuant to paragraphs 1 and 2 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] , the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.".

Article 82

Amendment to Regulation (EU) 2019/2144

In Article 11 of Regulation (EU) 2019/2144, the following paragraph is added:

"3. When adopting the implementing acts pursuant to paragraph 2, concerning artificial intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.

---

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …).”.

Article 82 a
Better regulation

In taking into account the requirements of this Regulation pursuant to the Amendments in Articles 75, 76, 77, 78, 79, 80, 81, and 82, the Commission shall conduct an analysis and consult relevant stakeholders to determine potential gaps as well as overlaps between existing sectoral legislation and the provisions of this Regulation.

Article 82b
Guidelines from the Commission on the implementation of this Regulation

1. The Commission shall develop, in consultation with the AI office, guidelines on the practical implementation of this Regulation, and in particular on:

- ***(i) the application of the requirements referred to in Articles 8 - 15 and Article 28 to 28b;***
- ***(ii) the prohibited practices referred to in Article 5;***
- ***(iii) the practical implementation of the provisions related to substantial modification;***
- ***(iv) the practical circumstances where the output of an AI system referred to in Annex III would pose a significant risk of harm to the health, safety or fundamental rights of natural persons as referred to in Article 6, paragraph 2, including examples in relation to high risk AI systems referred to in Annex III;***
- ***(v) the practical implementation of transparency obligations laid down in Article 52;***
- ***(vi) the development of codes of conduct referred to in Article 69***
- ***(vii) the relationship of this Regulation with other relevant Union legislation, including as regards consistency in their enforcement.***
- ***(viii) the practical implementation of Article 12, 28b on environmental impact of foundation models and Annex IV 3(b), particularly the measurement and logging methods to enable calculations and reporting of the environmental impact of systems to comply with the obligations in this Regulation, including carbon footprint and energy efficiency, taking into account state-of-the-art methods and economies of scale***

When issuing such guidelines, the Commission shall pay particular attention to the needs of SMEs including start-ups, local public authorities and sectors most likely to be affected by this Regulation.

2. Upon request of the Member States or the AI Office, or on its own initiative, the Commission shall update already adopted guidelines when deemed necessary.

Article 83
AI systems already placed on the market or put into service

1. ***Operators of*** the AI systems which are components of the large-scale IT systems established by the legal acts listed in Annex IX that have been placed on the market or put into service ***prior to ... [the date of entry into force of this Regulation] shall take the necessary steps to comply with the requirements laid down in this Regulation by [4 years after the date of entry into force of this Regulation]***

   The requirements laid down in this Regulation shall be taken into account in the evaluation of each large-scale IT systems established by the legal acts listed in Annex IX to be undertaken as provided for in those respective acts ***and whenever those legal acts are replaced or amended***.

2. This Regulation shall apply to ***operators of*** high-risk AI systems, other than the ones referred to in paragraph 1, that have been placed on the market or put into service before [*date of application of this Regulation referred to in Article 85(2)*], only if, from that date, those systems are subject to ***substantial modifications as defined in Article 3(23***). ***In the case of high-risk AI systems*** intended ***to be used by public authorities, providers and deployers of such systems shall take the necessary steps to comply with the requirements of the present Regulation within 2 years of its entry into force***.

Article 84
Evaluation and review

1. ***After consulting the AI Office,*** the Commission shall assess the need for amendment of the list in Annex III***, including the extension of existing area headings or addition of new area headings in that Annex; the list of prohibited AI practices in Article 5, and the list of AI systems requiring additional transparency measures in Article 52 (***once a year following the entry into force of this Regulation ***and following a recommendation of the AI Office)***. ***The Commission shall submit the findings of that assessment to the European Parliament and the Council.***

2. By [**two** *years after the date of application of this Regulation referred to in Article 85(2)*] and every ***two*** years thereafter, the Commission, ***together with the AI office,*** shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.

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

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

   (b) the state of penalties, and notably administrative fines as referred to in Article 71(1), applied by Member States to infringements of the provisions of this Regulation

   (ba) the level of the development of harmonised standards and common specifications for Artificial Intelligence

   (bb) the levels of investments in research, development and application of AI systems throughout the Union;

(bc) the competitiveness of the aggregated European AI sector compared to AI sectors in third countries

(bd) the impact of the Regulation with regards to the resource and energy use, as well as waste production and other environmental impact

(be) the implementation of the Coordinated Plan on AI, taking into account the different level of progress among Member States and identifying existing barriers to innovation in AI.

(bf) the update of the specific requirements regarding the sustainability of AI systems and foundation models, building on the reporting and documentation requirement in Annex IV and in Article 28b

(bg) the legal regime governing foundation models

(bh) the list of unfair contractual terms within Article 28a taking into account new business practices if necessary

3a. [2 year after the date of entry into application of this Regulation referred to in Article 85(2)] the Commission shall evaluate the functioning of the AI office, whether the office has been given sufficient powers and competences to fulfil its tasks and whether it would be relevant and needed for the proper implementation and enforcement of this Regulation to upgrade the Office and its enforcement competences and to increase its resources. The Commission shall submit this evaluation report to the European Parliament and to the Council.

4. Within [***one*** *year after the date of application of this Regulation referred to in Article 85(2)*] and every ***two*** years thereafter, the Commission shall evaluate the impact and effectiveness of codes of conduct to foster the application of the requirements set out in Title III, Chapter 2 and possibly other additional requirements for AI systems other than high-risk AI systems.

5. For the purpose of paragraphs 1 to 4 the ***AI Office*** , the Member States and national competent authorities shall provide the Commission with information on its request ***without undue delay***

6. In carrying out the evaluations and reviews referred to in paragraphs 1 to 4 the Commission shall take into account the positions and findings of ***the AI Office,*** of the European Parliament, of the Council, and of other relevant bodies or sources ***and shall consult relevant stakeholders. The result of such consultation shall be attached to the report.***

7. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account developments in technology ***the effect of AI systems on health and safety, fundamental rights, the environment, equality, and accessibility for persons with disabilities, democracy and rule of law*** and in the light of the state of progress in the information society.

7 a. To guide the evaluations and reviews referred to in paragraphs 1 to 4 of this Article, the Office shall undertake to develop an objective and participative methodology for the evaluation of risk level based on the criteria outlined in the relevant articles and inclusion of new systems in: the list in Annex III, including the extension of existing area headings or addition of new area headings in that Annex; the list of prohibited

practices laid down in Article 5; and the list of AI systems requiring additional transparency measures pursuant to Article 52.

7b. Any amendment to this Regulation pursuant to paragraph 7 of this Article, or relevant future delegated or implementing acts, which concern sectoral legislation listed in Annex II Section B, shall take into account the regulatory specificities of each sector, and existing governance, conformity assessment and enforcement mechanisms and authorities established therein.

7c. By five years from the date of application of this Regulation at the latest, the Commission shall carry out an assessment of the enforcement of this Regulation and shall report it to the European Parliament, the Council and the European Economic and Social Committee, taking into account the first years of application of the Regulation. On the basis of the findings that report shall, where appropriate, be accompanied by a proposal for amendment of this Regulation with regard to the structure of enforcement and the need for an EU agency to resolve any identified shortcomings.

Article 85
Entry into force and application

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

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

3. By way of derogation from paragraph 2:

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

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

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

Title VI, Chapter 1 and recital 76	**CA 8**

(76) In order to ***avoid fragmentation, to ensure the optimal functioning of the Single market, to*** ensure effective and harmonised implementation of this Regulation***, to achieve a high level of trustworthiness and of protection of health, safety, fundamental rights, the environment, democracy and the rule of law across the Union with regards to*** Artificial Intelligence ***systems, to actively support national supervisory authorities, Union institutions, bodies, offices and agencies in matters pertaining to this Regulation, and to increase the uptake of artificial intelligence throughout the Union, an European Union Artificial Intelligence Office*** should be established. The ***AI Office should have legal personality, should act in full independence, should be responsible for a number of advisory and coordination tasks, including issuing opinions, recommendations, advice or guidance on matters related to the implementation of this Regulation and should be adequately funded and staffed. Member States should provide the strategic direction and control of the AI Office through the management b***oard ***of the AI Office, alongside the Commission, the EDPS, the FRA, and ENISA. An executive director should be responsible for managing the activities of the secretariat of the AI office and for representing the AI office. Stakeholders should formally participate in the work of the AI Office through an advisory forum that should ensure varied and balanced stakeholder representation and should advise the AI Office on matters pertaining to. In case the establishment of the AI Office prove not to be sufficient to ensure a fully consistent application of this Regulation at Union level as well as efficient cross-border enforcement measures, the creation of an AI agency should be considered.***

TITLE VI

GOVERNANCE

CHAPTER 1

EUROPEAN ARTIFICIAL INTELLIGENCE *OFFICE*

SECTION 1: General provisions on the European Artificial Intelligence Office

Article 56
Establishment of the European Artificial Intelligence ***Office***

1. The 'European Artificial Intelligence Office' (the 'AI Office') is hereby established. The AI Office shall be an independent body of the Union. It shall have legal personality.

2. The AI Office shall have a secretariat, and shall be adequately funded and staffed for the purpose of performing its tasks pursuant to this Regulation.

3. The seat of the AI Office shall be in Brussels.

Article 56a
Structure

The administrative and management structure of the AI Office shall comprise:

(a) a management board, including a chair

(b) a secretariat managed by an executive director;

(c) an advisory forum.

Article 56b
Tasks of the AI Office
The AI Office shall carry out the following tasks:

a) support, advise, and cooperate with Member States, national supervisory authorities, the Commission and other Union institutions, bodies, offices and agencies with regard to the implementation of this Regulation;

b) monitor and ensure the effective and consistent application of this Regulation, without prejudice to the tasks of national supervisory authorities;

c) contribute to the coordination among national supervisory authorities responsible for the application of this Regulation~~,~~

d) serve as a mediator in discussions about serious disagreements that may arise between competent authorities regarding the application of the Regulation

e) coordinate joint investigations, pursuant to Article 66a;

f) contribute to the effective cooperation with the competent authorities of third countries and with international organisations.

g) collect and share ***Member State's*** expertise and best practices ***and to assist Member States national supervisory authorities and the Commission in developing the organizational and technical expertise required for the implementation of this Regulation, including by means of facilitating the creation and maintenance of a Union pool of experts***

h) examine, on its own initiative or upon the request of its management board or the Commission, questions relating to the implementation of this Regulation and to issue opinions, recommendations or written contributions including with regard to:

(i) technical specifications or existing standards;

(ii) the Commission's guidelines

(iii) codes of conduct and the application thereof, in close cooperation with industry and other relevant stakeholders;

(iv) the possible revision of the Regulation, the preparation of the delegated acts, and possible alignments of this Regulation with the legal acts listed in Annex II;

(v) trends, such as European global competitiveness in artificial intelligence, the uptake of artificial intelligence in the Union, the development of digital skills, and emerging systemic threats relating to artificial intelligence

(vi) guidance on how this Regulation applies to the ever evolving typology of AI value chains, in particular on the resulting implications in terms of accountability of all the entities involved

i) issue:

(i) an annual report that includes an evaluation of the implementation of this Regulation, a review of serious incident reports as referred to in Article 62 and the functioning of the database referred to in Article 60 and

(ii) recommendations to the Commission on the categorisation of prohibited practices, high-risk AI systems referred to in Annex III, the codes of conduct referred to in Article 69, and the application of the general principles outlines in Article 4a

j) assist authorities in the establishment and development of regulatory sandboxes and to facilitate cooperation among regulatory sandboxes;

k) organize meetings with Union agencies and governance bodies whose tasks are related to artificial intelligence and the implementation of this Regulation;

l) organize quarterly consultations with the advisory forum, and, where appropriate, public consultations with other stakeholders, and to make the results of those consultations public on its website;

m) promote public awareness and understanding of the benefits, risks, safeguards and rights and obligations in relation to the use of AI systems;

n) facilitate the development of common criteria and a shared understanding among market operators and competent authorities of the relevant concepts provided for in this Regulation;

o) provide monitoring of foundation models and to organise a regular dialogue with the developers of foundation models with regard to their compliance as well as AI systems that make use of such AI models

p) provide interpretive guidance on how the AI Act applies to the ever evolving typology of AI value chains, and what the resulting implications in terms of

accountability of all the entities involved will be under the different scenarios based on the generally acknowledged state of the art, including as reflected in relevant harmonized standards;

q) provide particular oversight and monitoring and institutionalize regular dialogue with the providers of foundation models about the compliance of foundation models as well as AI systems that make use of such AI models with Article 28b of this Regulation, and about industry best practices for self-governance. Any such meeting shall be open to national supervisory authorities, notified bodies and market surveillance authorities to attend and contribute;

r) issue and periodically update guidelines on the thresholds that qualify training a foundation model as a large training run, record and monitor known instances of large training runs, and issue an annual report on the state of play in the development, proliferation, and use of foundation models alongside policy options to address risks and opportunities specific to foundation models.

s) promote AI literacy pursuant to Article 4b.

Article 56c
Accountability, independence, and transparency

1. The AI Office shall:

a. be accountable to the European Parliament and to the Council in accordance with this Regulation;

b. act independently when carrying out its tasks or exercising its powers; and

c. ensure a high level of transparency concerning its activities and develop good administrative practices in that regard.

Regulation (EC) No 1049/2001 shall apply to documents held by the AI Office.

SECTION 2: Management board

Article 57b

Composition of the management board

1. The management board shall be composed of the following members:
(a) one representative of each Member State's national supervisory authority;
(b) one representative from the Commission
(c) one representative from the European Data Protection Supervisor (EDPS);

(d) one representative from the European Union Agency for Cybersecurity (ENISA);

(e) one representative from the Fundamental Rights Agency (FRA).

Each representative of a national supervisory authority shall have one vote. The representatives of the Commission, the EDPS, the ENISA and the FRA shall not have voting rights. Each member shall have a substitute. The appointment of members and substitute members of the management board shall take into account the need to gender balance. The members of the management board and their substitute members shall be made public.

2. The members and substitutes members of the management board shall not hold conflicting positions or commercial interests with regard to ~~in~~ any topic related to the application of the this Regulation.

3. The rules for the meetings and voting of the management board and the appointment and removal of the Executive Director shall be laid down in the rules of procedure referred to in Article 57c, point (a).

Article 57b
Functions of the management board

1. The management board shall have the following tasks:

(a) to make strategic decisions on the activities of the AI Office and to adopt its rules of procedure by a two-thirds majority of its members;
(b) to implement its rules of procedure;
(c) to adopt the AI Office's single programming document as well as it annual public report and transmit both to the European Parliament, to the Council, to the Commission, and to the Court of Auditors;
(d) to adopt the AI Office's budget;
(e) to appoint the executive director and, where relevant, to extend or curtail the executive director's term of office or remove him or her from office;
(f) to decide on the establishment of the AI Office's internal structures and, where necessary, the modification of those internal structures necessary for the fulfilment of the AI Office tasks;

Article 57c
Chair of the management board

1. The management board shall elect a Chair and two deputy Chairs from among its voting members, by simple majority.

2. The term of office of the Chair and of the deputy Chairs shall be four years. The terms of the Chair and of the deputy Chairs~~,~~ renewable once.

SECTION 2: Secretariat

Article 57

Secretariat

1. *The activities of the secretariat shall be managed by an executive director, who shall be accountable for his or her activities to the management board. Without prejudice to the respective powers of the management board and the Union institutions the executive director shall neither seek nor take instructions from any government or from any other body*

2. *The executive director shall attend hearings on any matter linked to the AI Office's activities and shall report on the performance of the executive director's duties when invited to do so by the European Parliament or the Council.*

3. *The executive director shall represent the AI Office, including in international fora for cooperation with regard to artificial intelligence;*

4. *The secretariat shall provide the management board and the advisory forum with the analytical, administrative and logistical support necessary to fulfil the tasks of the AI Office, including by:*

   (a) Implementing the decisions, programmes and activities adopted by the management board;

   (b) preparing each year the draft single programming document, the draft budget, the annual activity report on the AI Office, the draft opinions and positions of the AI Office, and submit them to the management board;

   (c) Coordinating with international fora for cooperation on artificial intelligence;

SECTION 4: Advisory Forum

Article 58
Advisory forum

1. *The advisory forum shall provide the AI Office with stakeholder input in matters relating to this Regulation, in particular with regard to the tasks set out in Article 56f point (b).*

2. *The membership of the advisory forum shall represent a balanced selection of stakeholders, including industry, start-ups, SMEs, civil society, the social partners and academia. The membership of the advisory forum shall be balanced with regard to commercial and non-commercial interests and, within the category of commercial interests, with regards to SMEs and other undertakings.*

3. The management board shall appoint the members of the advisory forum in accordance with the selection procedure established in the AI Office's rules of procedure and taking into account the need for transparency and in accordance with the criteria set out in paragraph 2;

4. The term of office of the members of the advisory forum shall be two years, which may be extended by up to no more than four years.

5. The European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC), and the European Telecommunications Standards Institute (ETSI) shall be permanent members of the Advisory Forum. The Joint Research Centre shall be permanent member, without voting rights.

6. The advisory forum shall draw up its rules of procedure. It shall elect two co-Chairs from among its members, in accordance with criteria set out in paragraph 2. The term of office of the co-Chairs shall be two years, renewable once.

7. The advisory forum shall hold meetings at least four times a year. The advisory forum may invite experts and other stakeholders to its meetings. The executive director may attend, ex officio, the meetings of the advisory forum.

8. In fulfilling its role as set out in paragraph 1, the advisory forum may prepare opinions, recommendations- and written contributions.

9. The advisory forum may establish standing or temporary subgroups as appropriate for the purpose of examining specific questions related to the objectives of this Regulation.

10. The advisory forum shall prepare an annual report of its activities. That report shall be made publicly available.

SECTION 5: European authorities on benchmarking

Article 58a
Benchmarking

The European authorities on benchmarking referred to in Article 15 (1a) and the AI Office shall, in close cooperation with international partners, jointly develop cost-effective guidance and capabilities to measure and benchmark aspects of AI systems and AI components, and notably of foundation models relevant to the compliance and enforcement of this Regulation based on the generally acknowledged state of the art, including as reflected in relevant harmonized standards.

Title VI, Chapter 2, Title VII, Title VIII and recitals 77-80a and 82-82b	**CA 9**

(77) ***Each*** Member State should designate ***a*** national ***supervisory authority*** for the purpose of supervising the application and implementation of this Regulation. ***It should also represent its Member State at the Management Board of the AI Office.*** 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 Union levels. ***Each*** national supervisory authority ***should act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.***

(77a) The national supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union. For that purpose, the national supervisory authorities should cooperate with each other, with therelevant national competent authorities, the Commission and with the AI Office.

(77b) The member or the staff of each national supervisory authority should, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, that duty of professional secrecy should in particular apply to trade secrets and to reporting by natural persons of infringements of this Regulation

(78) In order to ensure that providers of high-risk AI systems can take into account the experience on the use of high-risk AI systems for improving their systems and the design and development process or can take any possible corrective action in a timely manner, all providers should have a post-market monitoring system in place. This system is also key to ensure that the possible risks emerging from AI systems which continue to 'learn' ***or evolve*** after being placed on the market or put into service can be more efficiently and timely addressed. In this context, providers should also be required to have a system in place to report to the relevant authorities any serious incidents or any breaches to national and Union law***, including those*** protecting fundamental rights ***and consumer rights*** resulting from the use of their AI systems ***and take appropriate corrective actions***. ***Deployers should also report to the relevant authorities, any serious incidents or breaches to national and Union law resulting from the use of their AI system when they become aware of such serious incidents or breaches.***

(79) In order to ensure an appropriate and effective enforcement of the requirements and obligations set out by this Regulation, which is Union harmonisation legislation, the system of market surveillance and compliance of products established by Regulation (EU) 2019/1020 should apply in its entirety. ***For the purpose of this Regulation, national supervisory authorities should act as market surveillance authorities for AI systems covered by this Regulation except for AI systems covered by Annex II of this Regulation. For AI systems covered by legal acts listed in the Annex II, the competent authorites under those legal acts should remain the lead authority. National supervisory authorities and competent authorities in the legislation listed in Annex II should work together whenever necessary. When appropriate, the competent***

authorities in the legislation listed in Annex II should send competent staff to the national supervisory authority in order to assist in the performance of its tasks. For the purpose of this Regulation, national supervisory authorities should have the same powers and obligations as market surveillance authorities under Regulation (EU) 2019/1020. Where necessary for their mandate, national public authorities or bodies, which supervise the application of Union law protecting fundamental rights, including equality bodies, should also have access to any documentation created under this Regulation. ***After having exhausted all other reasonable ways to assess/verify the conformity and upon a reasoned request, the national supervisory authority should be granted access to the training, validation and testing datasets, the trained and training model of the high-risk AI system, including its relevant model parameters and their execution /run environment. In cases of simpler software systems falling under this Regulation that are not based on trained models, and where all other ways to verify conformity have been exhausted, the national supervisory authority may exceptionally have access to the source code, upon a reasoned request. Where the national supervisory authority has been granted access to the training, validation and testing datasets in accordance with this Regulation, such access should be achieved through appropriate technical means and tools, including on site access and in exceptional circumstances, remote access. The national supervisory authority should treat any information, including source code, software, and data as applicable, obtained as confidential information and respect relevant Union law on the protection of intellectual property and trade secrets. The national supervisory authority should delete any information obtained upon the completion of the investigation.***

(80) Union legislation on financial services includes internal governance and risk management rules and requirements which are applicable to regulated financial institutions in the course of provision of those services, including when they make use of AI systems. In order to ensure coherent application and enforcement of the obligations under this Regulation and relevant rules and requirements of the Union financial services legislation, the ***competent*** authorities responsible for the supervision and enforcement of the financial services legislation, including where applicable the European Central Bank should be designated as competent authorities for the purpose of supervising the implementation of this Regulation, including for market surveillance activities, as regards AI systems provided or used by regulated and supervised financial institutions. To further enhance the consistency between this Regulation and the rules applicable to credit institutions regulated under Directive 2013/36/EU of the European Parliament and of the Council[7], it is also appropriate to integrate the conformity assessment procedure and some of the providers' procedural obligations in relation to risk management, post marketing monitoring and documentation into the existing obligations and procedures under Directive 2013/36/EU. In order to avoid overlaps, limited derogations should also be envisaged in relation to the quality management system of providers and the monitoring obligation placed on ***deployers*** of high-risk AI systems to the extent that these apply to credit institutions regulated by Directive 2013/36/EU.

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

(80a) Given the objectives of this Regulation, namely to ensure an equivalent level of protection of health, safety and fundamental rights of natural persons, to ensure the protection of the rule of law and democracy, and taking into account that the mitigation of the risks of AI system against such rights may not be sufficiently achieved at national level or may be subject to diverging interpretation which could ultimately lead to an uneven level of protection of natural persons and create market fragmentation, the national supervisory authorities should be empowered to conduct joint investigations or rely on the union safeguard procedure provided for in this Regulation for effective enforcement. Joint investigations should be initiated where the national supervisory authority have sufficient reasons to believe that an infringement of this Regulation amount to a widespread infringement or a widespread infringement with a Union dimension, or where the AI system or foundation model presents a risk which affects or is likely to affect at least 45 million individuals in more than one Member State.

(82) It is important that AI systems related to products that are not high-risk in accordance with this Regulation and thus are not required to comply with the requirements set out ***for high-risk AI systems*** are nevertheless safe when placed on the market or put into service. To contribute to this objective, the Directive 2001/95/EC of the European Parliament and of the Council would apply as a safety net.

(84a) As the rights and freedoms of natural and legal persons and groups of natural persons can be seriously undermined by AI systems, it is essential that natural and legal persons or groups of natural persons have meaningful access to reporting and redress mechanisms and to be entitled to access proportionate and effective remedies. They should be able to report infringments of this Regulation to their national supervisory authority and have the right to lodge a complaint against the providers or deployers of AI systems. Where applicable, deployers should provide internal complaints mechanisms to be used by natural and legal persons or groups of natural persons. Without prejudice to any other administrative or non-judicial remedy, natural and legal persons and groups of natural persons should also have the right to an effective judicial remedy with regard to a legally binding decision of a national supervisory authority concerning them or, where the national supervisory authority does not handle a complaint, does not inform the complainant of the progress or preliminary outcome of the complaint lodged or does not comply with its obligation to reach a final decision, with regard to the complaint.

(84b) Affected persons should always be informed that they are subject to the use of a high-risk AI system, when deployers use a high-risk AI system to assist in decision-making or make decisions related to natural persons. This information can provide a basis for affected persons to exercise their right to an explanation under this Regulation. When deployers provide an explanation to affected persons under this Regulation, they should take into account the level of expertise and knowledge of the average consumer or individual

(84c) Union legislation on the protection of whistleblowers (Directive (EU) 2019/1937) has full application to academics, designers, developers, project contributors, auditors, product managers, engineers and economic operators acquiring information on breaches of Union law by a provider of AI system or its AI system.

CHAPTER 2

NATIONAL COMPETENT AUTHORITIES

Article 59
*Designation of national **supervisory** authorities*

1. Each Member State ***shall designate one national supervisory authority, which*** shall be organised so as to safeguard the objectivity and impartiality of ***its*** activities and tasks ***by [3 months after the entry into force of this Regulation]***. ***2. The*** national supervisory authority ***shall ensure the application and implementation of this Regulation. With regard to high-risk AI systems, related to products to which legal acts listed in Annex II apply, the*** competent authorities ***designated under those legal acts shall continue to lead the administrative procedures. However, to the extent a case involves aspects exclusively covered by this Regulation, those competent authorities shall be bound by the measures related to those aspects issued by the national supervisory authority designated under this Regulation.*** The national supervisory authority shall act as market surveillance authority. 3. Member States shall ***make publicly available and communicate to the AI Office and the*** Commission the ***national supervisory authority and information on how it can be contacted, by...[three months after the entry into force of this Regulation]. The national supervisory authority shall act as single point of contact for this Regulation and should be contactable though electronic communications means.***

4. Member States shall ensure that ***the*** national ***supervisory authority is*** provided with adequate ***technical,*** financial and human resources***, and infrastructure*** to fulfil their tasks ***effectively*** under this Regulation. In particular, ***the national supervisory authority*** shall have a sufficient number of personnel permanently available whose competences and expertise shall include an in-depth understanding of artificial intelligence technologies, data and data computing, ***personal data protection, cybersecurity, competition law,*** fundamental rights, health and safety risks and knowledge of existing standards and legal requirements. ***Member States shall assess and, if deemed necessary, update competence and resource requirements referred to in this paragraph on an annual basis.***

4a. Each national supervisory authority shall exercise their powers and carry out their duties independently, impartially and without bias. The members of each national supervisory authority, in the performance of their tasks and exercise of their powers under this Regulation,shall neither seek nor take instructions from anybody

4b. National supervisory authorities shall satisfy the minimum cybersecurity requirements set out for public administration entities identified as operators of essential services pursuant to Directive XXXX/XX on measures for a high common level of cybersecurity across the Union (NIS 2), repealing Directive (EU) 2016/1148.

4 c . ***When performing their tasks, the national supervisory authority shall act in compliance with the confidentiality obligations set out in Article 70.***

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

6. ~~T***he AI Office*** shall facilitate the exchange of experience between national competent ***supervisory*** authorities.~~

7. National ***supervisory*** authorities may provide guidance and advice on the implementation of this Regulation, including to ***SMEs and start-ups ,taking into account the AI Office or the Commission's guidance and advice .*** Whenever ***the*** national ***supervisory*** authorit***y***~~ies~~ intend to provide guidance and advice with regard to an AI system in areas covered by other Union legislation, the ***guidance shall be drafted in consultation with the*** competent national authorities under that Union legislation, as appropriate. ~~Member States may also establish one central contact point for communication with operators~~

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

Article 59a
Cooperation mechanism between national supervisory authorities in cases involving two or more Member States

1. Each national supervisory authority shall perform its tasks and powers conferred on in accordance with this Regulation on the territory of its own Member State.

2. In the event of a case involving two or more national supervisory authorities, the national supervisory authority of the Member State where the infringement took place shall be considered the lead supervisory authority.

3. In the cases referred to in paragraph 2, the relevant supervisory authorities shall cooperate and exchange all relevant information in due time. National supervisory authorities shall cooperate in order to reach a consensus.

TITLE VII

EU DATABASE FOR ~~STAND-ALONE~~ HIGH-RISK AI SYSTEMS

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

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

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

2a. The data listed in Annex VIII, Section B, shall be entered into the EU database by the deployers who are or who act on behalf of public authorities or Union institutions, bodies, offices or agencies and by deployers who are undertakings referred to in Article 51(1a) and (1b).

3. Information contained in the EU database shall be ***freely available*** to the public***, user-friendly and accessible, easily navigable and machine-readable containing structured digital data based on a standardised protocol***.

4. The EU database shall contain personal data only insofar as necessary for collecting and processing information in accordance with this Regulation. That information shall include the names and contact details of natural persons who are responsible for registering the system and have the legal authority to represent the provider ***or the deployer which is a public authority or Union institution, body, office or agency or a deployer acting on their behalf or a deployer which is an undertaking referred to in Article 51(1a)(b) and (1b)***.

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

5a. The database shall comply with the accessibility requirements of Annex I to Directive 2019/882

TITLE VIII

POST-MARKET MONITORING, INFORMATION SHARING, MARKET SURVEILLANCE

CHAPTER 1

POST-MARKET MONITORING

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

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

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

including other devices and software taking into account the rules applicable from areas such as data protection, intellectual property rights and competition law.

3. The post-market monitoring system shall be based on a post-market monitoring plan. The post-market monitoring plan shall be part of the technical documentation referred to in Annex IV. The Commission shall adopt an implementing act laying down detailed provisions establishing a template for the post-market monitoring plan and the list of elements to be included in the plan ***by [12 months following the entry into force]***.

4. For high-risk AI systems covered by the legal acts referred to in Annex II, where a post-market monitoring system and plan is already established under that legislation, the elements described in paragraphs 1, 2 and 3 shall be integrated into that system and plan as appropriate.

   The first subparagraph shall also apply to high-risk AI systems referred to in point 5(b) of Annex III placed on the market or put into service by credit institutions regulated by Directive 2013/36/EU.

CHAPTER 2

SHARING OF INFORMATION ON INCIDENTS AND MALFUNCTIONING

Article 62
Reporting of serious incidents ~~and of malfunctioning~~

1. Providers ***and, where deployers have identified a serious incident, deployers*** of high-risk AI systems placed on the Union market shall report any serious incident ~~or any malfunctioning~~ of those systems which constitutes a breach of obligations under Union law intended to protect fundamental rights to the ***national supervisory authority*** of the Member States where that incident or breach occurred.

   Such notification shall be made ~~,~~ ***without undue delay*** after the provider***, or where applicable the deployer,*** has established a causal link between the AI system and the incident ~~or malfunctioning~~ or the reasonable likelihood of such a link, and, in any event, not later than ~~15 days~~ ***72 hours (***after the providers~~, ~~***, or, where applicable, the deployer*** becomes aware of the serious incident~~or of the malfunctioning.~~

1a. Upon establishing a causal link between the AI system and the serious incident or the reasonable likelihood of such a link, providers shall take appropriate corrective actions pursuant to Article 21.

2. Upon receiving a notification related to a breach of obligations under Union law intended to protect fundamental rights, the ***national supervisory authority*** shall inform the national public authorities or bodies referred to in Article 64(3). The Commission shall develop dedicated guidance to facilitate compliance with the obligations set out in paragraph 1. That guidance shall be issued ***by [***the entry into force of this Regulation***]~~,~~ and shall be assessed regularly.***

2a. The national supervisory authority shall take appropriate measures within 7 days from the date it received the notification referred to in paragraph 1. Where the infringement takes place or is likely to take place in other Member States, the national

supervisory authority shall notify the AI Office and the relevant national supervisory authorities of these Member States.

3. For high-risk AI systems ***referred to in Annex III that*** are placed on the market or put into service by providers that are ***subject to Union legislative instruments laying down reporting obligations equivalent to those set out in this*** Regulation the notification of serious incidents constitut***ing*** a breach of ***fundamental rights under*** Union law ***shall be transferred to the national supervisory authority***

3a. National supervisory authorities shall on an annual basis notify the AI Office of the serious incidents reported to them in accordance with this Article.

CHAPTER 3

ENFORCEMENT

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

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

   (a) any reference to an economic operator under Regulation (EU) 2019/1020 shall be understood as including all operators identified in Title III, Chapter 3 of this Regulation;

   (b) any reference to a product under Regulation (EU) 2019/1020 shall be understood as including all AI systems falling within the scope of this Regulation.

   (ba) the national supervisory authorities shall act as market surveillance authorities under this Regulation and have the same powers and obligations as market surveillance authorities under Regulation (EU) 2019/1020.

2. The national supervisory authority shall report to the Commission ***and the AI Office annually*** the outcomes of relevant market surveillance activities. The national supervisory authority shall report, without delay, to the Commission and relevant national competition authorities any information identified in the course of market surveillance activities that may be of potential interest for the application of Union law on competition rules.

3. For high-risk AI systems, related to products to which legal acts listed in Annex II, section A apply, the market surveillance authority for the purposes of this Regulation shall be the authority responsible for market surveillance activities designated under those legal acts.

3a. For the purpose of ensuring effective enforcement of this Regulation, national supervisory authorities may:

(a) Carry out unannounced on-site and remote inspections of high-risk AI systems;

(b) Acquire samples related to high-risk AI systems, including through remote inspections, to reverse-engineer the AI systems and to acquire evidence to identify non-compliance.

4. For AI systems placed on the market, put into service or used by financial institutions regulated by Union legislation on financial services, the market surveillance authority for the purposes of this Regulation shall be the relevant authority responsible for the financial supervision of those institutions under that legislation.

5. For AI systems ***that*** are used for law enforcement purposes~~, points 6 and 7 of Annex III,~~ Member States shall designate as market surveillance authorities for the purposes of this Regulation ~~either~~ the competent data protection supervisory authorities under Directive (EU) 2016/680~~, or Regulation 2016/679 or the national competent authorities supervising the activities of the law enforcement, immigration or asylum authorities putting into service or using these systems.~~

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

7. ***National supervisory authorities*** designated under this Regulation ***shall coordinate with*** other relevant national authorities or bodies which supervise the application of Union harmonisation legislation listed in Annex II or other Union legislation that might be relevant for the high-risk AI systems referred to in Annex III.

Article 64
Access to data and documentation

1. ***I***n the context of their activities, ***and upon reasoned request*** the***national supervisory authority*** shall be granted full access to the training, validation and testing datasets used by the provider, ***or, where relevant, the deployer, that are relevant and strictly necessary for the purpose of its request*** through ~~application programming interfaces ('API') or other~~ appropriate technical means and tools ~~enabling remote access~~.

2. Where necessary to assess the conformity of the high-risk AI system with the requirements set out in Title III, Chapter 2***, after all other reasonable ways to verify conformity including paragraph 1 have been exhausted and have proven to be insufficient,*** and upon a reasoned request, the ***national supervisory authority*** shall be granted access to the training ***and trained*** models of the AI system, ***including its relevant model parameters***. ***All information in line with Article 70 obtained shall be treated as confidential information and shall be subject to existing Union law on the protection of intellectual property and trade secrets and shall be deleted upon the completion of the investigation for which the information was requested***.

2a. Paragraph 1 and 2 are without prejudice to the procedural rights of the concerned operator in accordance with Article 18 of Regulation (EU) 2019/1020.3. National public authorities or bodies which supervise or enforce the respect of obligations under Union law protecting fundamental rights in relation to the use of high-risk AI systems referred to in Annex III shall have the power to request and access any documentation created or maintained under this Regulation when access to that documentation is necessary for the fulfilment of the competences under their mandate within the limits of their jurisdiction. The relevant public authority or body

shall inform the ***national supervisory authority*** of the Member State concerned of any such request.

4. By 3 months after the entering into force of this Regulation, each Member State shall identify the public authorities or bodies referred to in paragraph 3 and make a list publicly available on the website of the national supervisory authority. ***National supervisory authorities*** shall notify the list to the Commission, ***the AI Office,*** and all other ***national supervisory authorities*** and keep the list up to date. ***The Commission shall publish in a dedicated website the list of all the competent authorities designated by the Member States in accordance with this article.***

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

6. Any information and documentation obtained by the national public authorities or bodies referred to in paragraph 3 pursuant to the provisions of this Article shall be treated in compliance with the confidentiality obligations set out in Article 70.

Article 65

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

1. AI systems presenting a risk shall be understood as ***an AI system having the potential to affect adversely*** health and safety, fundamental rights of persons ***in general, including in the workplace, protection of consumers, the environment, public security, or democracy or the rule of lawand other public interests, that are protected by the applicable Union harmonisation legislation, to a degree which goes beyond that considered reasonable and acceptable in relation to its intended purpose or under the normal or reasonably foreseeable conditions of use of the system*** are concerned***, including the duration of use and, where applicable, its putting into service, installation and maintenance requirements.***

2. Where the ***national supervisory authority*** of a Member State has sufficient reasons to consider that an AI system presents a risk as referred to in paragraph 1, ***it*** shall carry out an evaluation of the AI system concerned in respect of its compliance with all the requirements and obligations laid down in this Regulation. When risks to ~~the protection of~~ fundamental rights are present, the ***national supervisory authority*** shall also ***immediately*** inform ***and fully cooperate with*** the relevant national public authorities or bodies referred to in Article 64(3). ***Where there is sufficient reason to consider that that an AI system exploits the vulnerabilities of vulnerable groups or violates their rights intentionally or unintentionally, the national supervisory authority shall have the duty to investigate the design goals, data inputs, model selection, implementation and outcomes of the AI system .*** The relevant operators shall cooperate as necessary with the ***national supervisory authority*** and the other national public authorities or bodies referred to in Article 64(3).

Where, in the course of that evaluation, the ***national supervisory authority or, where relevant, the national public authority referred to in Article 64(3)*** finds that the AI system does not comply with the requirements and obligations laid down in this

Regulation, it shall without delay require the relevant operator to take all appropriate corrective actions to bring the AI system into compliance, to withdraw the AI system from the market, or to recall it within a reasonable period, commensurate with the nature of the risk, as it may prescribe ***and in any case no later than 15 working days or as provided for in the relevant Union harmonisation legislation as applicable***

The ***national supervisory 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 ***national supervisory authority*** considers that non-compliance is not restricted to its national territory, it shall inform the Commission***, the AI Office*** and the ***national supervisory authority of the*** other Member States ***without undue delay*** of the results of the evaluation and of the actions which it has required the operator to take.

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

5. Where the operator of an AI system does not take adequate corrective action within the period referred to in paragraph 2, the ***national supervisory authority*** shall take all appropriate provisional measures to prohibit or restrict the AI system's being made available on its national market ***or put into service,*** to withdraw the ***AI system*** from that market or to recall it. That authority shall ***immediately*** inform the Commission***, the AI Office*** and the ***national supervisory authority of*** 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 ***and the supply chain***, the nature of the non-compliance alleged and the risk involved, the nature and duration of the national measures taken and the arguments put forward by the relevant operator. In particular, the ***national supervisory authority*** shall indicate whether the non-compliance is due to one or more of the following:

   (a) a failure of the ***high-risk*** AI system to meet requirements set out in ***this Regulation***;

   (b) shortcomings in the harmonised standards or common specifications referred to in Articles 40 and 41 conferring a presumption of conformity.

   (ba) non-compliance with the prohibition of the artificial intelligence practices referred to in Article 5;

   (bb) non-compliance with provisions set out in Article 52

7. The ***national supervisory*** authorities of the Member States other than the ***national supervisory*** authority of the Member State initiating the procedure shall without delay inform the Commission***, the AI Office*** 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 national supervisory authority of*** a Member State or the Commission in respect of a provisional measure taken by a ***national supervisory authority of another*** Member State, that measure shall be deemed justified. This is without prejudice to the procedural rights of the concerned operator in accordance with Article 18 of Regulation (EU) 2019/1020. ***The period referred to in the first sentence of this paragraph shall be reduced to 30 days in the case of non-compliance with the prohibition of the artificial intelligence practices referred to in Article 5.***

9. The ***national supervisory authorities*** of all Member States shall ensure that appropriate restrictive measures are taken in respect of the ***AI system*** concerned, such as withdrawal of the ***AI system*** from their market, without delay.

9a. National supervisory authorities shall annually report to the AI Office about the use of prohibited practices that occurred during that year and about the measures taken to eliminate or mitigate the risks in accordance with this Article.

Article 66
Union safeguard procedure

1. Where, within three months of receipt of the notification referred to in Article 65(5), ***or 30 days in the case of non-compliance with the prohibition of the artificial intelligence practices referred to in Article 5,*** objections are raised by ***the national supervisory authority of*** a Member State against a measure taken by another ***national supervisory authority***, ***or in cases referred to in Article 59a(4),*** or where the Commission considers the measure to be contrary to Union law, the Commission shall without delay enter into consultation with the ***national supervisory authority of the*** relevant Member State and operator or operators and shall evaluate the national measure. On the basis of the results of that evaluation, the Commission shall decide whether the national measure is justified or not within ***three*** months***, or 60 days in the case of non-compliance with the prohibition of the artificial intelligence practices referred to in Article 5, starting*** from the notification referred to in Article 65(5) and notify such decision to ***the national supervisory authority of*** the Member State concerned. ***The Commission shall also inform all other national supervisory authorities of such decision.***

2. If the national measure is considered justified, all ***national supervisory authorities designated under this Regulation*** shall take the measures necessary to ensure that the non-compliant AI system is withdrawn from their market ***without delay,*** and shall inform the Commission ***and the AI Office*** accordingly. If the national measure is considered unjustified, the ***national supervisory authority of 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 40 and 41 of this Regulation, the Commission shall apply the procedure provided for in Article 11 of Regulation (EU) No 1025/2012.

.

Article 66 a
Joint investigations

1. Where a national supervisory authority has reasons to suspect that the infringement by a provider or a deployer of a high-risk AI system or foundation model to this Regulation amount to a widespread infringement with a Union dimension, or affects or is likely affect at least 45 million individuals, in more than one Member State, that national supervisory authority shall inform the AI Office and may request the national supervisory authorities of the Member States where such infringement took place to start a joint investigation. The AI Office shall provide central coordination to the joint investigation. Investigation powers shall remain within the competence of the national supervisory authorities.

Article 67
Compliant AI systems which present a risk

1. Where, having performed an evaluation under Article 65, ***in full cooperation with the relevant national public authority referred to in Article 64(3),*** the ***national supervisory authority*** of a Member State finds that although an AI system is in compliance with this Regulation, it presents a ***serious*** risk to the health or safety of persons, to the compliance with obligations under Union or national law intended to protect fundamental rights***, or the environment or the democracy and rule of law*** or to other aspects of public interest protection , it shall require the relevant operator to take all appropriate measures to ensure that the AI system concerned, when placed on the market or put into service, no longer presents that risk~~., to withdraw the AI system from the market or to recall it within a reasonable period, commensurate with the nature of the risk, as it may prescribe.~~

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

2a. Where the provider or other relevant operators fail to take corrective action as referred to in paragraph 2 and the AI system continues to present a risk as referred to in paragraph 1, the national supervisory authority may require the relevant operator to withdraw the AI system from the market or to recall it within a reasonable period, commensurate with the nature of the risk.~~.~~

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

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

5. The ***Commission, in consultation with the AI Office*** shall ***immediately communicate*** its decision to the ***national supervisory authorities of the*** Member States ***concerned***

and to the relevant operators. It shall also inform the decision to all other national supervisory authorities.

5a. The Commission shall adopt guidelines to help national competent authorities to identify and rectify, where necessary, similar problems arising in other AI systems.

Article 68
Formal non-compliance

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

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

   (b) the ***CE*** marking has not been affixed;

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

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

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

   (ea) the technical documentation is not available;

   (eb) the registration in the EU database has not been carried out.

   (ec) where applicable, the authorised representative has not been appointed.

2. Where the non-compliance referred to in paragraph 1 persists, the ***national supervisory authority of the*** Member State concerned shall take ~~all~~ appropriate ***and proportionate*** 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 ***without delay. The national supervisory authority of the Member State concerned shall immediately inform the AI Office of the non-compliance and the measures taken***.

Chapter 3a Remedies

Article 68a

Right to lodge a complaint with a national supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every natural persons or groups of natural persons shall have the right to lodge a complaint with a national supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if they consider that the AI system relating to him or her infringes this Regulation.

2. The national supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

Article 68b

Right to an effective judicial remedy against a supervisory authority

1. *Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a national supervisory authority concerning them.*
2. *Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to a an effective judicial remedy where the national supervisory authority which is competent pursuant to Articles 59 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 68a.*
3. *Proceedings against a national supervisory authority shall be brought before the courts of the Member State where the national supervisory authority is established.*
4. *Where proceedings are brought against a decision of a national supervisory authority which was preceded by an opinion or a decision of the Commission in the union safeguard procedure, the supervisory authority shall forward that opinion or decision to the court.*

Article 68c
A right to explanation of individual decision-making

1. *Any affected person subject to a decision which is taken by the deployer on the basis of the output from an high-risk AI system which produces legal effects or similarly significantly affects him or her in a way that they consider to adversely impact their health, safety, fundamental rights, socio-economic well-being or any other of the rights deriving from the obligations laid down in this Regulation, shall have the right to request from the deployer clear and meaningful explanation pursuant to Article 13(1) on the role of the AI system in the decision-making procedure, the main parameters of the decision taken and the related input data.*

2. *Paragraph 1 shall not apply to the use of AI systems for which exceptions from, or restrictions to, the obligation under paragraph 1 follow from Union or national law are provided in so far as such exception or restrictions respect the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society.*

3. *This Article shall apply without prejudice to Articles 13, 14, 15, and 22 of the Regulation 2016/679*

Article 68d

Representative actions

The following is added to Annex I of Directive (EU) 2020/1828 on Representative actions for the protection of the collective interests of consumers: "Regulation

xxxx/xxxx of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts".

Article 68e
Reporting of breaches and protection of reporting persons

Directive (EU) 2019/1937 of the European Parliament and of the Council shall apply to the reporting of breaches of this Regulation and the protection of persons reporting such breaches.

Title III, Chapter 1, Annexes II and III and recitals 27 to 41a	**CA 10**

(27) High-risk AI systems should only be placed on the Union market***,*** put into service ***or used*** if they comply with certain mandatory requirements. Those requirements should ensure that high-risk AI systems available in the Union or whose output is otherwise used in the Union do not pose unacceptable risks to important Union public interests as recognised and protected by Union law, ***including fundamental rights, democracy, the rule or law or the environment. In order to ensure alignment with sectoral legislation and avoid duplications, requirements for high-risk AI systems should take into account sectoral legislation laying down requirements for high-risk AI systems included in the scope of this Regulation, such as Regulation (EU) 2017/745 on Medical Devices and Regulation (EU) 2017/746 on In Vitro Diagnostic Devices or Directive 2006/42/EC on Machinery.*** AI systems identified as high-risk should be limited to those that have a significant harmful impact on the health, safety and fundamental rights of persons in the Union and such limitation minimises any potential restriction to international trade, if any. ***Given the rapid pace of technological development, as well as the potential changes in the use of AI systems, the list of high-risk areas and use-cases in Annex III should nonetheless be subject to permanent review through the exercise of regular assessment.***

(28) AI systems could ***have an*** adverse ***impact*** to health and safety of persons, in particular when such systems operate as ***safety*** components of products. Consistently with the objectives of Union harmonisation legislation to facilitate the free movement of products in the internal market and to ensure that only safe and otherwise compliant products find their way into the market, it is important that the safety risks that may be generated by a product as a whole due to its digital components, including AI systems, are duly prevented and mitigated. For instance, increasingly autonomous robots, whether in the context of manufacturing or personal assistance and care should be able to safely operate and perform their functions in complex environments. Similarly, in the health sector where the stakes for life and health are particularly high, increasingly sophisticated diagnostics systems and systems supporting human decisions should be reliable and accurate.

(28a) The extent of the adverse impact caused by the AI system on the fundamental rights protected by the Charter is of particular relevance when classifying an AI system as high-risk. Those rights include the right to human dignity, respect for private and family life, protection of personal data, freedom of expression and information, freedom of assembly and of association, and non-discrimination, right to education consumer protection, workers' rights, rights of persons with disabilities, gender equality, intellectual property rights, right to an effective remedy and to a fair trial, right of defence and the presumption of innocence, right to good administration. In addition to those rights, it is important to highlight that children have specific rights as enshrined in Article 24 of the EU Charter and in the United Nations Convention on the Rights of the Child (further elaborated in the UNCRC General Comment No. 25 as regards the digital environment), both of which require consideration of the children's vulnerabilities and provision of such protection and care as necessary for their well-being. The fundamental right to a high level of environmental protection

enshrined in the Charter and implemented in Union policies should also be considered when assessing the severity of the harm that an AI system can cause, including in relation to the health and safety of persons or to the environment.

(29) As regards high-risk AI systems that are safety components of products, or which are themselves products or systems falling within the scope of Regulation (EC) No 300/2008 of the European Parliament and of the Council[8], Regulation (EU) No 167/2013 of the European Parliament and of the Council[9], Regulation (EU) No 168/2013 of the European Parliament and of the Council[10], Directive 2014/90/EU of the European Parliament and of the Council[11], Directive (EU) 2016/797 of the European Parliament and of the Council[12], Regulation (EU) 2018/858 of the European Parliament and of the Council[13], Regulation (EU) 2018/1139 of the European Parliament and of the Council[14], and Regulation (EU) 2019/2144 of the European Parliament and of the Council[15], it is appropriate to amend those acts to ensure that the Commission takes into account, on the basis of the technical and regulatory specificities of each sector, and without interfering with existing governance, conformity assessment***, market surveillance*** and enforcement mechanisms and authorities established therein, the mandatory requirements for high-risk AI systems laid down in this Regulation when adopting any relevant future delegated or implementing acts on the basis of those acts.

(30) As regards AI systems that are safety components of products, or which are themselves products, falling within the scope of certain Union harmonisation legislation ***listed in Annex II of this Regulation,*** it is appropriate to classify them as high-risk under this

---

8 Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

9 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 (OJ L 60, 2.3.2013, p. 1).

10 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 (OJ L 60, 2.3.2013, p. 52).

11 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).

12 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 (OJ L 138, 26.5.2016, p. 44).

13 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 (OJ L 151, 14.6.2018, p. 1).

14 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 (OJ L 212, 22.8.2018, p. 1).

15 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 (OJ L 325, 16.12.2019, p. 1).

Regulation if the product in question undergoes the conformity assessment procedure ***in order to ensure compliance with essential safety requirements*** with a third-party conformity assessment body pursuant to that relevant Union harmonisation legislation. In particular, such products are machinery, toys, lifts, equipment and protective systems intended for use in potentially explosive atmospheres, radio equipment, pressure equipment, recreational craft equipment, cableway installations, appliances burning gaseous fuels, medical devices, and in vitro diagnostic medical devices.

(31) The classification of an AI system as high-risk pursuant to this Regulation should not ~~necessarily~~ mean that the product whose safety component is the AI system, or the AI system itself as a product, is considered 'high-risk' under the criteria established in the relevant Union harmonisation legislation that applies to the product. This is notably the case for Regulation (EU) 2017/745 of the European Parliament and of the Council[16] and Regulation (EU) 2017/746 of the European Parliament and of the Council[17], where a third-party conformity assessment is provided for medium-risk and high-risk products.

(32) As regards stand-alone AI systems, meaning high-risk AI systems other than those that are safety components of products, or which are themselves products ***and that are listed in one of the areas and use cases in Annex III***, it is appropriate to classify them as high-risk if, in the light of their intended purpose, they pose a ***significant*** risk of harm to the health and safety or the fundamental rights of persons ***and, where the AI system is used as a safety component of a critical infrastructure, to the environment . Such significant risk of harm should be identified by assessing on the one hand the effect of such risk with respect to its level of severity, intensity, probability of occurrence and duration combined altogether and on the other hand whether the risk can affect an individual, a plurality of persons or a particular group of persons. Such combination could for instance result in a high severity but low probability to affect a natural person, or a high probability to affect a group of persons with a low intensity over a long period of time, depending on the context.*** The identification of those systems is based on the same methodology and criteria envisaged also for any future amendments of the list of high-risk AI systems.

(32a) Providers whose AI systems fall under one of the areas and use cases listed in Annex III that consider their system does not pose a significant risk of harm to the health, safety, fundamental rights or the environment should inform the national supervisory authorities by submitting a reasoned notification. This could take the form of a one-page summary of the relevant information on the AI system in question, including its intended purpose and why it would not pose a significant risk of harm to the health, safety, fundamental rights or the environment. The Commission should specify criteria to enable companies to assess whether their system would pose such risks, as well as develop an easy to use and standardised template for the notification. Providers should submit the notification as early as possible and in any case prior to the placing of the AI system on the market or its putting into service, ideally at the development stage, and they should be free to place it on the market at any given time

---

16 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).

17 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).

after the notification. However, if the authority estimates the AI system in question was misclassified, it should object to the notification within a period of three months. The objection should be substantiated and duly explain why the AI system has been misclassified. The provider should retain the right to appeal by providing further arguments. If after the three months there has been no objection to the notification, national supervisory authorities could still intervene if the AI system presents a risk at national level, as for any other AI system on the market. National supervisory authorities should submit annual reports to the AI Office detailing the notifications received and the decisions taken.

(33) ~~Technical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to biased results and entail discriminatory effects. This is particularly relevant when it comes to age, ethnicity, sex or disabilities. Therefore, 'real-time' and 'post' remote biometric identification systems should be classified as high-risk. In view of the risks that they pose, both types of remote biometric identification systems should be subject to specific requirements on logging capabilities and human oversight.~~

(33) As biometric data constitute a special category of sensitive personal data in accordance with Regulation 2016/679, it is appropriate to classify as high-risk several critical use-cases of biometric and biometrics-based systems. AI systems intended to be used for biometric identification of natural persons and AI systems intended to be used to make inferences about personal characteristics of natural persons on the basis of biometric or biometrics-based data, including emotion recognition systems, with the exception of those which are prohibited under this Regulation should therefore be classified as high-risk. This should not include AI systems intended to be used for biometric verification, which includes authentication, whose sole purpose is to confirm that a specific natural person is the person he or she claims to be and to confirm the identity of a natural person for the sole purpose of having access to a service, a device or premises (one-to-one verification). Biometric and biometrics-based systems which are foreseen under EU law to enable cybersecurity and personal data protection measures should not be considered as posing a significant risk of harm to the health, safety and fundamental rights.

(34) As regards the management and operation of critical infrastructure, it is appropriate to classify as high-risk the AI systems intended to be used as safety components in the management and operation of the supply of water, gas, heating electricity ***and critical digital infrastructure***, since their failure or malfunctioning may ***infringe the security and integrity of such critical infrastructure or*** put at risk the life and health of persons at large scale and lead to appreciable disruptions in the ordinary conduct of social and economic activities. ***Safety components of critical infrastructure, including critical digital infrastructure, are systems used to directly protect the physical integrity of physical infrastructure or health and safety of persons and property. Failure or malfunctioning of such components might directly lead to risks to the physical integrity of critical infrastructure and thus to risks to health and safety of persons and property. Components intended to be used solely for cybersecurity purposes should not qualify as safety components. Examples of such safety components may include systems for monitoring water pressure or fire alarm controlling systems in cloud computing centres.***

(35) ***Deployment of AI systems in education is important in order to help modernise entire education systems, to increase educational quality, both offline and online and to accelerate digital education, thus also making it available to a broader audience .*** AI systems used in education or vocational training, notably for determining access ***or materially influence decisions on admission*** or assigning persons to educational and vocational training institutions or to evaluate persons on tests as part of or as a precondition for their education ***or to assess the appropriate level of education for an individual and materially influence the level of education and training that individuals will receive or be able to access or to monitor and detect prohibited behaviour of students during tests*** should be ***classified as*** high-risk ***AI systems***, since they may determine the educational and professional course of a person's life and therefore affect their ability to secure their livelihood. When improperly designed and used, such systems ***can be particularly intrusive and*** may violate the right to education and training as well as the right not to be discriminated against and perpetuate historical patterns of discrimination, ***for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation***.

(36) AI systems used in employment, workers management and access to self-employment, notably for the recruitment and selection of persons, for making decisions ***or materially influence decisions*** on ***initiation,*** promotion and termination and for ***personalised*** task allocation ***based on individual behaviour, personal traits or biometric data,*** monitoring or evaluation of persons in work-related contractual relationships, should also be classified as high-risk, since those systems may appreciably impact future career prospects, livelihoods of these persons ***and workers' rights***. Relevant work-related contractual relationships should ***meaningfully*** involve employees and persons providing services through platforms as referred to in the Commission Work Programme 2021. Throughout the recruitment process and in the evaluation, promotion, or retention of persons in work-related contractual relationships, such systems may perpetuate historical patterns of discrimination, for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation. AI systems used to monitor the performance and behaviour of these persons may also ***undermine the essence of their fundamental*** impact their rights to data protection and privacy. ***This Regulation applies without prejudice to Union and Member State competences to provide for more specific rules for the use of AI-systems in the employment context.***

(37) Another area in which the use of AI systems deserves special consideration is the access to and enjoyment of certain essential private and public services, ***including healthcare services, and essential services, including but not limited to housing, electricity, heating/cooling and internet,*** and benefits necessary for people to fully participate in society or to improve one's standard of living. In particular, AI systems used to evaluate the credit score or creditworthiness of natural persons should be classified as high-risk AI systems, since they determine those persons' access to financial resources or essential services such as housing, electricity, and telecommunication services. AI systems used for this purpose may lead to discrimination of persons or groups and perpetuate historical patterns of discrimination, for example based on racial or ethnic origins, ***gender,*** disabilities, age, sexual orientation, or create new forms of discriminatory impacts. ***However, AI systems foreseen by Union law for the purpose of detecting fraud in the offering of financial services should not be considered as***

high-risk under this Regulation. Natural persons applying for or receiving public assistance benefits and services from public authorities***, including healthcare services and essential services, including but not limited to housing, electricity, heating/cooling and internet,*** are typically dependent on those benefits and services and in a vulnerable position in relation to the responsible authorities. If AI systems are used for determining whether such benefits and services should be denied, reduced, revoked or reclaimed by authorities, they may have a significant impact on persons' livelihood and may infringe their fundamental rights, such as the right to social protection, non-discrimination, human dignity or an effective remedy. Similarly, AI systems intended to be used ***to make decisions or materially influence decisions on the eligibility of natural persons for health and life insurance may also have a significant impact on persons' livelihood and may infringe their fundamental rights such as by limiting access to healthcare or by perpetuating discrimination based on personal characteristics.*** Those systems should therefore be classified as high-risk. Nonetheless, this Regulation should not hamper the development and use of innovative approaches in the public administration, which would stand to benefit from a wider use of compliant and safe AI systems, provided that those systems do not entail a high risk to legal and natural persons. Finally, AI systems used ***to evaluate and classify emergency calls by natural persons or*** to dispatch or establish priority in the dispatching of emergency first response services should also be classified as high-risk since they make decisions in very critical situations for the life and health of persons and their property.

(37a) Given the role and responsibility of police and judicial authorities, and the impact of decisions they take for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, some specific use-cases of AI applications in law enforcement has to be classified as high-risk, in particular in instances where there is the potential to significantly affect the lives or the fundamental rights of individuals.

(38) Actions by law enforcement authorities involving certain uses of AI systems are characterised by a significant degree of power imbalance and may lead to surveillance, arrest or deprivation of a natural person's liberty as well as other adverse impacts on fundamental rights guaranteed in the Charter. In particular, if the AI system is not trained with high quality data, does not meet adequate requirements in terms of its ***performance, its*** accuracy or robustness, or is not properly designed and tested before being put on the market or otherwise put into service, it may single out people in a discriminatory or otherwise incorrect or unjust manner. Furthermore, the exercise of important procedural fundamental rights, such as the right to an effective remedy and to a fair trial as well as the right of defence and the presumption of innocence, could be hampered, in particular, where such AI systems are not sufficiently transparent, explainable and documented. It is therefore appropriate to classify as high-risk a number of AI systems intended to be used in the law enforcement context where accuracy, reliability and transparency is particularly important to avoid adverse impacts, retain public trust and ensure accountability and effective redress. In view of the nature of the activities in question and the risks relating thereto, those high-risk AI systems should include in particular AI systems intended to be used by ***or on behalf of*** law enforcement authorities ***or by Union agencies, offices or bodies in support of law***

enforcement authorities, as polygraphs and similar tools ***insofar as their use is permitted under relevant Union and national law,*** for the evaluation of the reliability of evidence in criminal proceedings, for profiling in the course of detection, investigation or prosecution of criminal offences, as well as for crime analytics regarding natural persons. AI systems specifically intended to be used for administrative proceedings by tax and customs authorities should not be ***classified as*** high-risk AI systems used by law enforcement authorities for the purposes of prevention, detection, investigation and prosecution of criminal offences. ***The use of AI tools by law enforcement and judicial authorities should not become a factor of inequality, social fracture or exclusion. The impact of the use of AI tools on the defence rights of suspects should not be ignored, notably the difficulty in obtaining meaningful information on their functioning and the consequent difficulty in challenging their results in court, in particular by individuals under investigation.***

(39) AI systems used in migration, asylum and border control management affect people who are often in particularly vulnerable position and who are dependent on the outcome of the actions of the competent public authorities. The accuracy, non-discriminatory nature and transparency of the AI systems used in those contexts are therefore particularly important to guarantee the respect of the fundamental rights of the affected persons, notably their rights to free movement, non-discrimination, protection of private life and personal data, international protection and good administration. It is therefore appropriate to classify as high-risk AI systems intended to be used by ***or on behalf of*** competent public authorities ***or by Union agencies, offices or bodies*** charged with tasks in the fields of migration, asylum and border control management as polygraphs and similar tools ***insofar as their use is permitted under relevant Union and national law,*** for assessing certain risks posed by natural persons entering the territory of a Member State or applying for visa or asylum; for verifying the authenticity of the relevant documents of natural persons; for assisting competent public authorities for the examination ***and assessment of the veracity of evidence in relation to*** applications for asylum, visa and residence permits and associated complaints with regard to the objective to establish the eligibility of the natural persons applying for a status; ***for monitoring, surveilling or processing personal data in the context of border management activities, for the purpose of detecting, recognising or identifying natural persons; for the forecasting or prediction of trends related to migration movements and border crossings***. AI systems in the area of migration, asylum and border control management covered by this Regulation should comply with the relevant procedural requirements set by the Directive 2013/32/EU of the European Parliament and of the Council49, the Regulation (EC) No 810/2009 of the European Parliament and of the Council50 and other relevant legislation. ***The use of AI systems in migration, asylum and border control management should in no circumstances be used by Member States or Union institutions, agencies or bodies as a means to circumvent their international obligations under the Convention of 28 July 1951 relating to the Status of Refugees as amended by the Protocol of 31 January 1967, nor should they be used to in any way infringe on the principle of non-refoulement, or or deny safe and effective legal avenues into the territory of the Union, including the right to international protection***.

(40) Certain AI systems intended for the administration of justice and democratic processes should be classified as high-risk, considering their potentially significant impact on democracy, rule of law, individual freedoms as well as the right to an effective remedy

and to a fair trial. In particular, to address the risks of potential biases, errors and opacity, it is appropriate to qualify as high-risk AI systems intended to ***be used by a judicial authority or administrative body or on their behalf to*** assist judicial authorities ***or administrative bodies*** in researching and interpreting facts and the law and in applying the law to a concrete set of facts ***or used in a similar way in alternative dispute resolution***. ***The use of artificial intelligence tools can support, but should not replace the decision-making power of judges or judicial independence, as the final decision-making must remain a human-driven activity and decision.*** Such qualification should not extend, however, to AI systems intended for purely ancillary administrative activities that do not affect the actual administration of justice in individual cases, such as anonymisation or pseudonymisation of judicial decisions, documents or data, communication between personnel, administrative tasks or allocation of resources***.***

(40a) In order to address the risks of undue external interference to the right to vote enshrined in Article 39 of the Charter, and of disproportionate effects on democratic processes, democracy, and the rule of law, AI systems intended to be used to influence the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda should be classified as high-risk AI systems. with the exception of AI systems whose output natural persons are not directly exposed to, such as tools used to organise, optimise and structure political campaigns from an administrative and logistic point of view.

(40b) Considering the scale of natural persons using the services provided by social media platforms designated as very large online platforms, such online platforms can be used in a way that strongly influences safety online, the shaping of public opinion and discourse, election and democratic processes and societal concerns. It is therefore appropriate that AI systems used by those online platforms in their recommender systems are subject to this Regulation so as to ensure that the AI systems comply with the requirements laid down under this Regulation, including the technical requirements on data governance, technical documentation and traceability, transparency, human oversight, accuracy and robustness. Compliance with this Regulation should enable such very large online platforms to comply with their broader risk assessment and risk-mitigation obligations in Article 34 and 35 of Regulation EU 2022/2065. The obligations in this Regulation are without prejudice to Regulation (EU) 2022/2065 and should complement the obligations required under the Regulation (EU) 2022/2065 when the social media platform has been designated as a very large online platform. Given the European-wide impact of social media platforms designated as very large online platforms, the authorities designated under Regulation (EU) 2022/2065 should act as enforcement authorities for the purposes of enforcing this provision.

(41) The fact that an AI system is classified ***as a*** high risk ***AI system*** under this Regulation should not be interpreted as indicating that the use of the system is necessarily lawful ***or unlawful*** under other acts of Union law or under national law compatible with Union law, such as on the protection of personal data, Any such use should continue to occur solely in accordance with the applicable requirements resulting from the Charter and from the applicable acts of secondary Union law and national law.

(41a) A number of legally binding rules at European, national and international level already apply or are relevant to AI systems today, including but not limited to EU

primary law (the Treaties of the European Union and its Charter of Fundamental Rights), EU secondary law (such as the General Data Protection Regulation, the Product Liability Directive, the Regulation on the Free Flow of Non-Personal Data, anti-discrimination Directives, consumer law and Safety and Health at Work Directives), the UN Human Rights treaties and the Council of Europe conventions (such as the European Convention on Human Rights), and numerous EU Member State laws. Besides horizontally applicable rules, various domain-specific rules exist that apply to particular AI applications (such as for instance the Medical Device Regulation in the healthcare sector).

TITLE III

HIGH-RISK AI SYSTEMS

CHAPTER 1

CLASSIFICATION OF AI SYSTEMS AS HIGH-RISK

Article 6
Classification rules for high-risk AI systems

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

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

   (b) the product whose safety component ***pursuant to point (a)*** is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment ***related to risks for health and safety,*** with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II.

2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems ***falling under one or more of the critical areas and use cases*** referred to in Annex III shallbe considered high-risk ***if they pose a significant risk of harm to the health, safety or fundamental rights of natural persons. Where an AI system falls under Annex III point 2, it shall be considered high-risk if it poses a significant risk of harm to the environment.***

   The Commission shall, 6 months prior to the entry into force of this Regulation, following consultation with the AI Office and relevant stakeholders, provide guidelines clearly specifying the circumstances where the output of AI systems referred to in Annex III would pose a significant risk of harm to the health, safety or fundamental rights of natural persons or cases in which it would not.

2a. Where providers falling under one or more of the critical areas and use cases referred to in Annex III consider that their AI system does not pose a significant risk as described in paragraph 2, they shall submit a reasoned notification to the National

Supervisory Authority that they are not subject to the requirements of Title III Chapter 2 of this Regulation. Where the AI system is intended to be used in two or more Member States, the aforementioned notification shall be addressed to the AI Office. Without prejudice to Article 65, the National Supervisory Authority shall review and reply, directly or via the AI Office, within 3 months if they deem the AI system to be misclassified.

2b. Providers that misclassify their AI system as not subject to the requirements of Title III Chapter 2 of this Regulation and place it on the market before the deadline for objection by National Supervisory Authorities shall be responsible and be subject to fines pursuant to Article 71.

2c. National supervisory authorities shall submit a yearly report to the AI Office detailing the number of notifications received, the related high-risk areas at stake and the decisions taken concerning received notifications

Article 7
Amendments to Annex III

1. The Commission is empowered to adopt delegated acts in accordance with Article 73 to ***amend*** Annex III by adding ***or modifying areas or use-cases of*** high-risk AI systems where ***these*** pose a ***significant*** risk of harm to health and safety, or ***an*** adverse impact on fundamental rights, ***to the environment, or to democracy and the rule of law, and*** that ***risk*** is***,*** in respect of its severity and probability of occurrence, equivalent to or greater than the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III.

1a. The Commission is also empowered to adopt delegated acts in accordance with Article 73 to remove use-cases of high-risk AI systems from the list in Annex III if the conditions referred to in paragraph 1 no longer apply

2. When assessing ***an AI system*** for the purposes of paragraph 1 ***and 1a*** the Commission shall take into account the following criteria:

   (a) the intended purpose of the AI system;

   (aa) the general capabilities and functionalities of the AI system independent of its intended purpose;

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

   (ba) the nature and amount of the data processed and used by the AI system;

   (bb) the extent to which the AI system actsautonomously;

   (c) the extent to which the use of an AI system has already caused harm to health and safety***, has had an*** adverse impact on fundamental rights, ***the environment, democracy and the rule of law*** or has given rise to significant concerns in relation to the ***likelihood*** of such harm or adverse impact, as demonstrated ***for example*** by reports or documented allegations submitted to national ***supervisory*** authorities***, to the Commission, to the AI Office, to the EDPS, or to the European Union Agency for Fundamental Rights***;

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

(e) the extent to which potentially harmed or adversely impacted persons are dependent on the ***output*** produced ***involving*** an AI system, ***and that output is purely accessory in respect of the relevant action or decision to be taken***, in particular because for practical or legal reasons it is not reasonably possible to opt-out from that ***output***;

(ea) the potential misuse and malicious use of the AI system and of the technology underpinning it;

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

(g) the extent to which the outcome produced ***involving*** an AI system is easily reversible ***or remedied***, whereby outcomes having an ***adverse*** impact on the health,safety***, fundamental rights*** of persons***, the environment, or on democracy and rule of law*** shall not be considered as easily reversible;

(ga) the extent of the availability and use of effectivetechnical solutions and mechanisms for the control, reliability and corrigibility of the AI system;

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

(gc) the extent of human oversight and the possibility for a human to intercede in order to override a decision or recommendations that may lead to potential harm;

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

(i) effective measures of redress in relation to the ***damage caused*** by an AI system, with the exclusion of claims for ***direct or indirect*** damages;

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

2a. When assessing an AI system for the purposes of paragraphs 1 or 1a the Commission shall consult the AI Office and, where relevant, representatives of groups on which an AI system has an impact, industry, independent experts, social partners, and civil society organisations. The Commission shall also organise public consultations in this regard and shall make the results of those consultations and of the final assessment publicly available.

2b. The AI Office, national supervisory authorities or the European Parliament may request the Commission to reassess the risk categorisation in accordance with paragraph 1 and 1a. The AI system shall then be reviewed for reassessment and may be re-categorized. The Commission shall give reasons for its decision and make them public.

Article 15
Accuracy, robustness and cybersecurity

1a. To address the technical aspects of how to measure the appropriate levels of accuracy and robustness set out in paragraph 1 of this Article, the AI Office shall bring together national and international metrology and benchmarking authorities and provide non-binding guidance on the matter as set out in Article 56, paragraph 2, point (a).

ANNEX II
LIST OF UNION HARMONISATION LEGISLATION
Section A – List of Union harmonisation legislation based on the New Legislative Framework

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) [as repealed by the Machinery Regulation];

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

3. Directive 2013/53/EU of the European Parliament and of the Council of 20 November 2013 on recreational craft and personal watercraft and repealing Directive 94/25/EC (OJ L 354, 28.12.2013, p. 90);

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

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

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

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

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

9. Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC (OJ L 81, 31.3.2016, p. 51);

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

11. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 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;

12. 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).

Section B. List of other Union harmonisation legislation

Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

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 (OJ L 60, 2.3.2013, p. 52);

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 (OJ L 60, 2.3.2013, p. 1);

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);

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 (OJ L 138, 26.5.2016, p. 44).

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 (OJ L 151, 14.6.2018, p. 1); 3. 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 (OJ L 325, 16.12.2019, p. 1);

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 (OJ L 212, 22.8.2018, p. 1), in so far as the design, production and placing on the market of aircrafts referred to in points (a) and (b) of Article 2(1) thereof, where it concerns

unmanned aircraft and their engines, propellers, parts and equipment to control them remotely, are concerned.

ANNEX III

HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(2)

The AI systems specifically mentioned under points 1-8a stand for critical use cases and are each considered to be high-risk AI systems pursuant to Article 6(2)***, provided that they fulfil the criteria set out in that Article***:

1. Biometric ***and biometrics-based systems***

   (a) AI systems intended to be used for-***biometric identification of natural persons, with the exception of those mentioned in Article 5;***

   (aa) AI systems intended to be used to make inferences about personal characteristics of natural persons on the basis of biometric or biometrics-based data, including emotion recognition systems, with the exception of those mentioned in Article 5;

   Point 1 shall not include AI systems intended to be used for biometric verification whose sole purpose is to confirm that a specific natural person is the person he or she claims to be.

2. Management and operation of critical infrastructure:

   (a) AI systems intended to be used as safety components in the management and operation of road, ***rail and air*** traffic ***unless these are regulated in harmonisation or sectoral legislation***.

   (aa) ***AI systems intended to be used as safety components in the management and operation of*** the supply of water, gas, heating, electricity ***and critical digital infrastructure***

3. Education and vocational training:

   (a) AI systems intended to be used for the purpose of determining access ***or materially influence decisions on admission*** or assigning natural persons to educational and vocational training institutions;

   (b) AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to ***those*** institutions***;***

   ba) systems intended to be used for the purpose of assessing the appropriate level of education for an individual and materially influencing the level of education and vocational training that individual will receive or will be able to access.

   bb) AI systems intended to be used for monitoring and detecting prohibited behaviour of students during tests in the context of/within education and vocational training institutions;

4. Employment, workers management and access to self-employment:

(a) AI systems intended to be used for recruitment or selection of natural persons, notably ***for placing targeted job advertisements,*** ~~,~~ screening or filtering applications, evaluating candidates in the course of interviews or tests;

(b) AI ***systems*** intended to be used ***to make or materially influence*** decisions ***affecting the initiation,*** promotion and termination of work-related contractual relationships, ***task allocation based on individual behaviour or personal traits or characteristics, or*** for monitoring and evaluating performance and behavior of persons in such relationships.

5. Access to and enjoyment of essential private services and public services and benefits:

(a) AI systems intended to be used by ***or on behalf of*** public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, ***including healthcare services and essential services, including but not limited to housing, electricity, heating/cooling and internet,*** as well as to grant, reduce, revoke, ***increase*** or reclaim such benefits and services;

(b) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score ***, with the exception of AI systems used for the purpose of detecting financial fraud*** ~~the exception of AI systems put into service by small scale providers for their own use~~;

(ba) AI systems intended to be used for making decisions or materially influencing decisions on the eligibility of natural persons for health and life insurance;

(c) AI systems intended ***to evaluate and classify emergency calls by natural persons or*** to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including ***by police and law enforcement,*** firefighters and medical aid***, as well as of emergency healthcare patient triage systems***.

6. Law enforcement:

~~(a) AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences;~~

(b) AI systems intended to be used by ***or on behalf of*** law enforcement authorities***, or by Union agencies, offices or bodies in support of law enforcement authorities*** as polygraphs and similar tools ; ***insofar as their use is permitted under relevant Union and national law***

~~(c) AI systems intended to be used by law enforcement authorities to detect deep fakes as referred to in article 52(3);~~

~~(d)~~ AI systems intended to be used by ***or on behalf of*** law enforcement authorities***, or by Union agencies, offices or bodies in support of law enforcement authorities to evaluate*** of the reliability of evidence in the course of investigation or prosecution of criminal offences;

~~(e) AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups;~~

~~(f)~~ AI systems intended to be used by ***or on behalf of*** law enforcement authorities ***or by Union agencies, offices or bodies in support of law enforcement authorities*** for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences ***or, in the case of Union agencies, offices or bodies, as referred to in Article 3(5) of Regulation (EU) 2018/1725***;

~~(g)~~ AI systems intended to be used ***by or on behalf of law enforcement authorities or by Union agencies, offices or bodies in support of law enforcement authorities*** for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data.

7. Migration, asylum and border control management:

(a) AI systems intended to be used by ***or on behalf of*** competent public authorities ***or by Union agencies, offices or bodies*** as polygraphs and similar tools ***insofar as their use is permitted under relevant Union or national law***

(b) AI systems intended to be used by ***or on behalf of*** competent public authorities ***or by Union agencies, offices or bodies*** to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State;

(c) AI systems intended to be used by ***or on behalf of*** competent public authorities ***or by Union agencies, offices or bodies*** for the verification of the authenticity of travel documents and supporting documentation of natural persons and detect non-authentic documents by checking their security features;

(d) AI systems intended to ***be used by or on behalf of competent public authorities or by Union agencies, offices or bodies to*** assist competent public authorities for the examination ***and assessment of the veracity of evidence in relation to*** applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status.

(da) ***AI systems intended to be used by or on behalf of competent public authorities or by Union agencies, offices or bodies in migration, asylum and border control management to monitor, surveil or process data in the context of border management activities, for the purpose of detecting, recognising or identifying natural persons***

(db) AI systems intended to be used by or on behalf of competent public authorities or by Union agencies, offices or bodies in migration, asylum and border control management for the forecasting or prediction of trends related to migration movement and border crossing

8. Administration of justice and democratic processes:

a) AI systems intended ***to be used by a judicial authority ot administrative body or on their behalf*** to assist a judicial authority ***or administrative body*** in researching and interpreting facts and the law and in applying the law to a concrete set of facts ***or used in a similar way in alternative dispute resolution***.

aa) AI systems intended to be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda

This does not include AI systems whose output natural persons are not directly exposed to, such as tools used to organise, optimise and structure political campaigns from an administrative and logistic point of view.

(ab) AI systems intended to be used by social media platforms that have been designated as very large online platforms within the meaning of Article 33 of Regulation EU 2022/2065, in their recommender systems to recommend to the recipient of the service user-generated content available on the platform.

Article 5(1)(a) to (c), (da) to (dc), Article 5(1a), recitals 14-17 and 26a-26d	**CA 11**

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

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

(16) The placing on the market, putting into service or use of certain AI systems ***with the objective to or the effect of materially distorting*** human behaviour, whereby physical or psychological harms are likely to occur, should be forbidden. ***This limitation should be understood to include neuro-technologies assisted by AI systems that are used to monitor, use, or influence neural data gathered through brain-computer interfaces insofar as they are materially distorting the behaviour of a natural person in a manner that causes or is likely to cause that person or another person significant harm.*** Such AI systems deploy subliminal components individuals cannot perceive or exploit vulnerabilities of ***individuals***-and ***specific groups of persons***-due to their ***known or predicted personality traits,*** age, physical or mental incapacities***, social or economic situation***. They do so with the intention to ***or the effect of*** materially ***distorting*** the behaviour of a person and in a manner that causes or is likely to cause ***significant*** harm to that or another person ***or groups of persons, including harms that may be accumulated over time.*** The intention ***to distort the behaviour*** may not be presumed if the distortion results from factors external to the AI system which are outside of the control of the provider or the user***, such as factors that may not be reasonably foreseen and mitigated by the provider or the deployer of the AI system. In any case, it is not necessary for the provider or the deployer to have the intention to cause the significant harm, as long as such harm results from the manipulative or exploitative AI-enabled practices. The prohibitions for such AI practices is complementary to the provisions contained in Directive [Unfair Commercial Practice Directive 2005/29/EC, as amended by Directive (EU) 2019/216], according to which unfair commercial practices are prohibited, irrespective of whether they carried out having recourse to AI systems or otherwise. In such setting, lawful commercial practices, for example in the field of advertising, that are in compliance with Union law should not in themselves be regarded as violating prohibition.*** Research for legitimate purposes in relation to such AI systems should not be stifled by the prohibition, if such research does not amount to use of the AI system in human-machine relations that exposes

natural persons to harm and such research is carried out in accordance with recognised ethical standards for scientific research ***and on the basis of specific informed consent of the individuals that are exposed to them or, where applicable, of their legal guardian.***

(16a) AI systems that categorise natural persons by assigning them to specific categories, according to known or inferred sensitive or protected characteristics are particularly intrusive, violate human dignity and hold great risk of discrimination. Such characteristics include gender, gender identity, race, ethnic origin, migration or citizenship status, political orientation, sexual orientation, religion, disability or any other grounds on which discrimination is prohibited under Article 21 of the EU Charter of Fundamental Rights, as well as under Article 9 of Regulation (EU)2016/769. Such systems should therefore be prohibited.

(17) AI systems providing social scoring of natural persons for general purpose may lead to discriminatory outcomes and the exclusion of certain groups. They violate the right to dignity and non-discrimination and the values of equality and justice. Such AI systems evaluate or classify natural persons ***or groups*** based on ***multiple data points and time occurrences related to*** their social behaviour in multiple contexts or known***, inferred*** or predicted personal or personality characteristics. The social score obtained from such AI systems may lead to the detrimental or unfavourable treatment of natural persons or whole groups thereof in social contexts, which are unrelated to the context in which the data was originally generated or collected or to a detrimental treatment that is disproportionate or unjustified to the gravity of their social behaviour. Such AI systems should be therefore prohibited.

(26a) AI systems used by law enforcement authorities or on their behalf to make predictions, profiles or risk assessments based on profiling of natural persons or data analysis based on personality traits and characteristics, including the person's location, or past criminal behaviour of natural persons or groups of persons for the purpose of predicting the occurrence or reoccurrence of an actual or potential criminal offence(s) or other criminalised social behaviour or administrative offences, including fraud-predicition systems, hold a particular risk of discrimination against certain persons or groups of persons, as they violate human dignity as well as the key legal principle of presumption of innocence. Such AI systems should therefore be prohibited.

(26b) The indiscriminate and untargeted scraping of biometric data from social media or CCTV footage to create or expand facial recognition databases add to the feeling of mass surveillance and can lead to gross violations of fundamental rights, including the right to privacy. The use of AI systems with this intended purpose should therefore be prohibited.

(26c) There are serious concerns about the scientific basis of AI systems aiming to detect emotions, physical or physiological features such as facial expressions, movements, pulse frequency or voice. Emotions or expressions of emotions and perceptions thereof vary considerably across cultures and situations, and even within a single individual. Among the key shortcomings of such technologies, are the limited reliability (emotion categories are neither reliably expressed through, nor unequivocally associated with, a common set of physical or physiological movements), the lack of specificity (physical or physiological expressions do not perfectly match emotion categories) and the limited generalisability (the effects of context and culture are not sufficiently considered). Reliability issues and

consequently, major risks for abuse, may especially arise when deploying the system in real-life situations related to law enforcement, border management, workplace and education institutions. Therefore, the placing on the market, putting into service, or use of AI systems intended to be used in these contexts to detect the emotional state of individuals should be prohibited.

(26d) Practices that are prohibited by Union legislation, including data protection law, non-discrimination law, consumer protection law, and competition law, should not be affected by this Regulation.

TITLE II

PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES

Article 5

1. The following artificial intelligence practices shall be prohibited:

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

The prohibition of an AI system that deploys subliminal techniques referred to in the first sub-paragraph shall not apply to AI systems intended to be used for approved therapeutical purposes on the basis of specific informed consent of the individuals that are exposed to them or, where applicable, of their legal guardian

(b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a ***person or*** a specific group of persons***, including characteristics of such individual's or group of persons' known or predicted personality traits or social or economic situation***, age, physical or mental ability, ***with the objective or to the effect of*** materially ***distorting*** the behaviour of ***that person or*** a person pertaining to that group in a manner that causes or is likely to cause that person or another person ***significant*** harm***;***

(***ba) the placing on the market, putting into service or use of biometric categorisation systems that categorise natural persons according to sensitive or protected attributes or characteristics or based on the inference of those attributes or characteristics. This prohibition shall not apply to AI systems intended to be used for approved therapeutical purposes on the basis of specific informed consent of the individuals that are exposed to them or, where applicable, of their legal guardian.***

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

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

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

(da) the placing on the market, putting into service or use of an AI system for making risk assessments of natural persons or groups thereof in order to assess the risk of a natural person for offending or reoffending or for predicting the occurrence or reoccurrence of an actual or potential criminal or administrative offence based on profiling of a natural person or on assessing personality traits and characteristics, including the person's location, or past criminal behaviour of natural persons or groups of natural persons;

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

(dc) the placing on the market, putting into service or use of AI systems to infer emotions of a natural person in the areas of law enforcement, border management, in workplace and education institutions.

1a. This Article shall not affect the prohibitions that apply where an artificial intelligence practice infringes another EU law, including EU acquis on data protection, non discrimination, consumer protection or competition.

Article 5(1)(d), Article 5(2) to (4), Article 5(1)(e) and recitals 18-26	**CA 11A**

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

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

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

(iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA62 and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State.

2. The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall take into account the following elements:

(a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system;

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

In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall comply with necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations

3. As regards paragraphs 1, point (d) and 2, each individual use for the purpose of law enforcement of a 'real-time' remote biometric identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or by an independent administrative authority of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 4. However, in a duly justified situation of urgency, the use of the system may be commenced without an authorisation and the authorisation may be requested only during or after the use. The competent judicial or administrative authority shall only grant the authorisation where it is satisfied, based on objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system at issue is necessary for and proportionate to achieving one of the objectives specified in paragraph 1, point (d), as identified in the request. In deciding on the request, the competent judicial or administrative authority shall take into account the elements referred to in paragraph 2.

4. A Member State may decide to provide for the possibility to fully or partially authorise the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement within the limits and under the conditions listed in paragraphs 1, point (d), 2 and 3. That Member State shall lay down in its national law the necessary detailed rules for the request, issuance and exercise of, as

~~well as supervision relating to, the authorisations referred to in paragraph 3. Those rules shall also specify in respect of which of the objectives listed in paragraph 1, point (d), including which of the criminal offences referred to in point (iii) thereof, the competent authorities may be authorised to use those systems for the purpose of law enforcement~~

(e) the putting into service or use of AI systems for the analysis of recorded footage of publicly accessible spaces through 'post' remote biometric identification systems, unless they are subject to a pre-judicial authorisation in accordance with Union law and strictly necessary for the targeted search connected to a specific serious criminal offense as defined in Article 83(1) of TFEU that already took place for the purpose of law enforcement.

(18) The use of AI systems for 'real-time' remote biometric identification of natural persons in publicly accessible spaces is particularly intrusive ***to*** the rights and freedoms of the concerned persons, ***and can ultimately*** affect the private life of a large part of the population, evoke a feeling of constant surveillance***, give parties deploying biometric identification in publicly accessible spaces a position of uncontrollable power*** and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights ***at the core to the Rule of Law. Technical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to biased results and entail discriminatory effects. This is particularly relevant when it comes to age, ethnicity, sex or disabilities.*** In addition, the immediacy of the impact and the limited opportunities for further checks or corrections in relation to the use of such systems operating in 'real-time' carry heightened risks for the rights and freedoms of the persons that are concerned by law enforcement activities. ***The use of those systems in publicly accessible places should therefore be prohibited. Similarly, AI systems used for the analysis of recorded footage of publicly accessible spaces through 'post' remote biometric identification systems should also be prohibited, unless there is pre-judicial authorisation for use in the context of law enforcement, when strictly necessary for the targeted search connected to a specific serious criminal offense that already took place, and only subject to a pre-judicial authorization.***

~~(19) The use of those systems for the purpose of law enforcement should therefore be prohibited, except in three exhaustively listed and narrowly defined situations, where the use is strictly necessary to achieve a substantial public interest, the importance of which outweighs the risks. Those situations involve the search for potential victims of crime, including missing children; certain threats to the life or physical safety of natural persons or of a terrorist attack; and the detection, localisation, identification or prosecution of perpetrators or suspects of the criminal offences referred to in Council Framework Decision 2002/584/JHA[18] if those criminal offences are punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years and as they are defined in the law of that Member State. Such threshold for the custodial sentence or detention order in accordance with national law contributes to ensure that the offence should be serious enough to potentially justify the use of 'real-time' remote biometric identification systems. Moreover, of the 32~~

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

criminal offences listed in the Council Framework Decision 2002/584/JHA, some are in practice likely to be more relevant than others, in that the recourse to 'real-time' remote biometric identification will foreseeably be necessary and proportionate to highly varying degrees for the practical pursuit of the detection, localisation, identification or prosecution of a perpetrator or suspect of the different criminal offences listed and having regard to the likely differences in the seriousness, probability and scale of the harm or possible negative consequences.

(20) In order to ensure that those systems are used in a responsible and proportionate manner, it is also important to establish that, in each of those three exhaustively listed and narrowly defined situations, certain elements should be taken into account, in particular as regards the nature of the situation giving rise to the request and the consequences of the use for the rights and freedoms of all persons concerned and the safeguards and conditions provided for with the use. In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement should be subject to appropriate limits in time and space, having regard in particular to the evidence or indications regarding the threats, the victims or perpetrator. The reference database of persons should be appropriate for each use case in each of the three situations mentioned above.

(21) Each use of a 'real-time' remote biometric identification system in publicly accessible spaces for the purpose of law enforcement should be subject to an express and specific authorisation by a judicial authority or by an independent administrative authority of a Member State. Such authorisation should in principle be obtained prior to the use, except in duly justified situations of urgency, that is, situations where the need to use the systems in question is such as to make it effectively and objectively impossible to obtain an authorisation before commencing the use. In such situations of urgency, the use should be restricted to the absolute minimum necessary and be subject to appropriate safeguards and conditions, as determined in national law and specified in the context of each individual urgent use case by the law enforcement authority itself. In addition, the law enforcement authority should in such situations seek to obtain an authorisation as soon as possible, whilst providing the reasons for not having been able to request it earlier.

(22) Furthermore, it is appropriate to provide, within the exhaustive framework set by this Regulation that such use in the territory of a Member State in accordance with this Regulation should only be possible where and in as far as the Member State in question has decided to expressly provide for the possibility to authorise such use in its detailed rules of national law. Consequently, Member States remain free under this Regulation not to provide for such a possibility at all or to only provide for such a possibility in respect of some of the objectives capable of justifying authorised use identified in this Regulation.

(23) The use of AI systems for 'real-time' remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement necessarily involves the processing of biometric data. The rules of this Regulation that prohibit, subject to certain exceptions, such use, which are based on Article 16 TFEU, should apply as *lex specialis* in respect of the rules on the processing of biometric data contained in Article 10 of Directive (EU) 2016/680, thus regulating such use and the processing of biometric data involved in an exhaustive manner. Therefore, such use and processing should only be possible in as far as it is compatible with the framework set by this Regulation, without there being scope, outside that framework, for the competent authorities, where

~~they act for purpose of law enforcement, to use such systems and process such data in connection thereto on the grounds listed in Article 10 of Directive (EU) 2016/680. In this context, this Regulation is not intended to provide the legal basis for the processing of personal data under Article 8 of Directive 2016/680. However, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for purposes other than law enforcement, including by competent authorities, should not be covered by the specific framework regarding such use for the purpose of law enforcement set by this Regulation. Such use for purposes other than law enforcement should therefore not be subject to the requirement of an authorisation under this Regulation and the applicable detailed rules of national law that may give effect to it.~~

(24) Any processing of biometric data and other personal data involved in the use of AI systems for biometric identification, other than in connection to the use of 'real-time' remote biometric identification systems in publicly accessible spaces ~~for the purpose of law enforcement~~ as regulated by this Regulation, ~~including where those systems are used by competent authorities in publicly accessible spaces for other purposes than law enforcement,~~ should continue to comply with all requirements resulting from Article 9(1) of Regulation (EU) 2016/679, Article 10(1) of Regulation (EU) 2018/1725 and Article 10 of Directive (EU) 2016/680, as applicable.

(25) In accordance with Article 6a of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the TEU and to the TFEU, Ireland is not bound by the rules laid down in Article 5(1), point (d), ~~(2) and (3~~) of this Regulation adopted on the basis of Article 16 of the TFEU which relate to the processing of personal data by the Member States when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU, where Ireland is not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16 of the TFEU.

(26) In accordance with Articles 2 and 2a of Protocol No 22 on the position of Denmark, annexed to the TEU and TFEU, Denmark is not bound by rules laid down in Article 5(1), point (d), ~~(2) and (3~~) of this Regulation adopted on the basis of Article 16 of the TFEU, or subject to their application, which relate to the processing of personal data by the Member States when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU.

Article 3 – paragraph 1 – points 1 to 44 i, 45 c to 45 f, Articles 4, 4a and 4d, Annex I and recitals 6 to 9b	**CA 12**

(6) The notion of AI system ***in this Regulation*** should be clearly defined ***and closely aligned with the work of international organisations working on artificial intelligence*** to ensure legal certainty***, harmonization and wide acceptance***, while providing the flexibility to accommodate ***the rapid*** technological developments ***in this field***. ***Moreover, it*** should be based on key characteristics of artificial intelligence, ***such as its learning, reasoning or modelling capabilities, so as to distinguish it from simpler software systems or programming approaches. AI systems are designed to operate with varying levels of autonomy, meaning that they have at least some degree of independence of actions from human controls and of capabilities to operate without human intervention. The term "machine-based" refers to the fact that AI systems run on machines. The reference to explicit or implicit objectives underscores that AI systems can operate according to explicit human-defined objectives or to implicit objectives. The objectives of the AI system may be different from the intended purpose of the AI system in a specific context. The reference to predictions includes content, which is considered in this Regulation a form of prediction as one of the possible outputs produced by an AI system. For the purposes of this Regulation, environments should be understood as the contexts in which the AI systems operate, whereas outputs generated by the AI system, meaning predictions, recommendations or decisions, respond to the objectives of the system, on the basis of inputs from said environment. Such output further influences said environment, even by merely introducing new information to it.***

(6a) AI systems often have machine learning capacities that allow them to adapt and perform new tasks autonomously. Machine learning refers to the computational process of optimizing the parameters of a model from data, which is a mathematical construct generating an output based on input data. Machine learning approaches include, for instance, supervised, unsupervised and reinforcement learning, using a variety of methods including deep learning with neural networks. This Regulation is aimed at addressing new potential risks that may arise by delegating control to AI systems, in particular to those AI systems that can evolve after deployment. The function and outputs of many of these AI systems are based on abstract mathematical relationships that are difficult for humans to understand, monitor and trace back to specific inputs. These complex and opaque characteristics (black box element) impact accountability and explainability. Comparably simpler techniques such as knowledge-based approaches, Bayesian estimation or decision-trees may also lead to legal gaps that need to be addressed by this Regulation, in particular when they are used in combination with machine learning approaches in hybrid systems.

(6b) AI systems can be used as stand-alone software system, integrated into a physical product (embedded), used to serve the functionality of a physical product without

being integrated therein (non-embedded) or used as an AI component of a larger system. If this larger system would not function without the AI component in question, then the entire larger system should be considered as one single AI system under this Regulation.

(7) The notion of biometric data used in this Regulation is in line with and should be interpreted consistently with the notion of biometric data as defined in Article 4(14) of Regulation (EU) 2016/679 of the European Parliament and of the Council. ***Biometrics-based data are additional data resulting from specific technical processing relating to physical, physiological or behavioural signals of a natural person, such as facial expressions, movements, pulse frequency, voice, key strikes or gait, which may or may not allow or confirm the unique identification of a natural person.***

(7a) The notion of biometric identification as used in this Regulation should be defined as the automated recognition of physical, physiological, behavioural, and psychological human features such as the face, eye movement, facial expressions, body shape, voice, speech, gait, posture, heart rate, blood pressure, odour, keystrokes, psychological reactions (anger, distress, grief, etc.) for the purpose of establishing an individual's identity by comparing biometric data of that individual to stored biometric data of individuals in a database (one-to-many identification), irrespective of whether the individual has given its consent or not.

(7b) The notion of biometric categorisation as used in this Regulation should be defined as assigning natural persons to specific categories or inferring their characteristics and attributes such as gender, sex, age, hair colour, eye colour, tattoos, ethnic or social origin, health, mental or physical ability, behavioural or personality, traits language, religion, or membership of a national minority or sexual or political orientation on the basis of their biometric or biometric-based data, or which can be inferred from such data

(8) The notion of remote biometric identification system as used in this Regulation should be defined functionally, as an AI system intended for the identification of natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge whether the targeted person will be present and can be identified, irrespectively of the particular technology, processes or types of biometric data used***, exlcuding verification systems which merely compare the biometric data of an individual to their previously provided biometric data (one-to-one)***. Considering their different characteristics and manners in which they are used, as well as the different risks involved, a distinction should be made between 'real-time' and 'post' remote biometric identification systems. In the case of 'real-time' systems, the capturing of the biometric data, the comparison and the identification occur all instantaneously, near-instantaneously or in any event without a significant delay. In this regard, there should be no scope for circumventing the rules of this Regulation on the 'real-time' use of the AI systems in question by providing for minor delays. 'Real-time' systems involve the use of 'live' or 'near-'live' material, such as video footage, generated by a camera or other device with similar functionality. In the case of 'post' systems, in contrast, the biometric data have already been captured and the comparison and identification occur only after a significant delay. This involves material, such as pictures or video footage generated by closed circuit television cameras or private devices, which has been generated before the use of the system in respect of the natural persons concerned. ***Given that the notion of biometric***

identification is independent from the individual's consent, this definition applies even when warning notices are placed in the location that is under surveillance of the remote biometric identification system, and is not de facto annulled by pre-enrolment.

(8a) The identification of natural persons at a distance is understood to distinguish remote biometric identification systems from close proximity individual verification systems using biometric identification means, whose sole purpose is to confirm whether or not a specific natural person presenting themselves for identification is permitted, such as in order to gain access to a service, a device, or premises.

(9) For the purposes of this Regulation the notion of publicly accessible space should be understood as referring to any physical place that is accessible to the public, irrespective of whether the place in question is privately or publicly owned ***and regardless of the potential capacity restrictions***. Therefore, the notion does not cover places that are private in nature and normally not freely accessible for third parties, including law enforcement authorities, unless those parties have been specifically invited or authorised, such as homes, private clubs, offices, warehouses and factories. Online spaces are not covered either, as they are not physical spaces. However, the mere fact that certain conditions for accessing a particular space may apply, such as admission tickets or age restrictions, does not mean that the space is not publicly accessible within the meaning of this Regulation. Consequently, in addition to public spaces such as streets, relevant parts of government buildings and most transport infrastructure, spaces such as cinemas, theatres, ***sports grounds, schools, universities, relevant parts of hospitals and banks, amusement parks, festivals,*** shops and shopping centres are normally also publicly accessible. Whether a given space is accessible to the public should however be determined on a case-by-case basis, having regard to the specificities of the individual situation at hand.

(9a) It is important to note that AI systems should make best efforts to respect general principles establishing a high-level framework that promotes a coherent human-centric approach to ethical and trustworthy AI in line with the Charter of Fundamental Rights of the European Union and the values on which the Union is founded, including the protection of fundamental rights, human agency and oversight, technical robustness and safety, privacy and data governance, transparency, non-discrimination and fairness and societal and environmental wellbeing

(9b) 'AI literacy' refers to skills, knowledge and understanding that allows providers, users and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause and thereby promote its democratic control. AI literacy should not be limited to learning about tools and technologies, but should also aim to equip providers and users with the notions and skills required to ensure compliance with and enforcement of this Regulation. It is therefore necessary that the Commission, the Member States as well as providers and users of AI systems, in cooperation with all relevant stakeholders, promote the development of a sufficient level of AI literacy, in all sectors of society, for people of all ages, including women and girls, and that progress in that regard is closely followed.

Article 3
Definitions

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

(1) 'artificial intelligence system' (AI system) means ***a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments.***

(1a) 'risk' means the combination of the probability of an occurrence of harm and the severity of that harm;

(1b) 'significant risk' means a risk that is significant as a result of the combination of its severity, intensity, probability of occurrence, and duration of its effects, and its the ability to affect an individual, a plurality of persons or to affect a particular group of persons;

(1c) 'foundation model' means an AI model that is trained on broad data at scale, is designed for generality of output, and can be adapted to a wide range of distinctive tasks;

(1d) 'general purpose AI system' means an AI system that can be used in and adapted to a wide range of applications for which it was not intentionally and specifically designed;

(1e) 'large training runs' means the production process of a powerful AI models that require computing resources above a very high threshold.

(2) 'provider' means a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge;

(3) ~~'small-scale provider' means a provider that is a micro or small enterprise within the meaning of Commission Recommendation 2003/361/E~~

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

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

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

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

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

(8a) ‘affected person’ means any natural person or group of persons who are subject to or otherwise affected by an AI system;

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

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

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

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

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

(14) ‘safety component of a product or system’ means, ***in line with Union harmonisation legislation listed in Annex II,*** a component of a product or of a system which fulfils a ***critical*** safety function for that product or system~~, or~~ the failure or malfunctioning of which endangers the health and safety of persons~~, or property~~

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

(16) ‘recall of an AI system’ means any measure aimed at achieving the return to the provider of an AI system ***that has been*** made available to ***deployers;***

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

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

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

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

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

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

(23) 'substantial modification' means a ***modification or a series of modifications of*** the AI system ***after*** its placing on the market or putting into service which ***is not foreseen or planned in the initial risk assessment by the provider and as a result of which*** the compliance of the AI system with the requirements set out in Title III, Chapter 2 of this Regulation ***is affected*** or results in a modification to the intended purpose for which the AI system has been assessed

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

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

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

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

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

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

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

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

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

(33) 'biometric data' means ***biometric data as defined in Article 4, point (14) of Regulation (EU) 2016/679;*** ~~personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;~~

(33a) 'biometric-based data' means data resulting from specific technical processing relating to physical, physiological or behavioural signals of a natural person;~~

(33b) 'biometric identification' means the automated recognition of physical, physiological, behavioural, and psychological human features for the purpose of establishing an individual's identity by comparing biometric data of that individual to stored biometric data of individuals in a database (one-to-many identification);

(33c) 'biometric verification' means the automated verification of the identity of natural persons by comparing biometric data of an individual to previously provided biometric data (one-to-one verification, including authentication)

(33e) 'special categories of personal data' means the categories of personal data referred to in Article 9(1) of Regulation (EU)2016/679;

(34) 'emotion recognition system' means an AI system for the purpose of identifying or inferring emotions***, thoughts, states of mind*** or intentions of ***individuals or groups*** on the basis of their biometric ***and biometric-based*** data;

(35) 'biometric categorisation means assigning natural persons to specific categories, ***or inferring their characteristics and attributes*** on the basis of their biometric ***or biometric-based*** data, ***or which can be inferred from such data***;

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

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

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

(39) 'publicly accessible space' means any ***publicly or privately owned*** physical place accessible to the public, regardless of whether certain conditions for access may apply***, and regardless of the potential capacity restrictions***;

(40) 'law enforcement authority' means:

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

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

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

(42) 'national supervisory authority' means ***a public*** authority to which a Member State assigns the responsibility for the implementation and application of this Regulation, for coordinating the activities entrusted to that Member State, for acting as the single contact point for the Commission, and for representing the Member State ***in the management*** Board ***of the AI Office***;

(43) 'national competent authority' means ***any of*** the national ***authorities which are responsible for the enforcement of this Regulation,***

(44) 'serious incident' means any incident ***or malfunctioning of an AI system*** that directly or indirectly leads, might have led or might lead to any of the following:

(a) the death of a person or serious damage to a person's health, ~~to property or the environment,~~
(b) a serious ~~and irreversible~~ disruption of the management and operation of critical infrastructure.
(ba) a breach of fundamental rights protected under Union law;
(bb) serious damage to property or the environment;

(44a) 'personal data' means personal data as defined in Article 4, point (1) of Regulation (EU)2016/679;

(44b) 'non-personal data' means data other than personal data;

(44c) 'profiling' means any form of automated processing of personal data as defined in point (4) of Article 4 of Regulation (EU) 2016/679; or in the case of law enforcement authorities – in point 4 of Article 3 of Directive (EU) 2016/680 or, in the case of Union institutions, bodies, offices or agencies, in point 5 Article 3 of Regulation (EU) 2018/1725;

(44d) 'deep fake' means manipulated or synthetic audio, image or video content that would falsely appear to be authentic or truthful, and which features depictions of persons appearing to say or do things they did not say or do, produced using AI techniques, including machine learning and deep learning; ~~.~~

(44e) 'widespread infringement' means:

(a) any act or omission contrary to Union law that protects the interests of individuals, that has harmed or is likely to harm the collective interests of individuals residing in at least two Member States other than the Member State, in which:

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

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

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

(b) any acts or omissions contrary to Union law that protects the interests of individuals, that have done, do or are likely to do harm to the collective interests of individuals and that have common features, including the same unlawful practice, the same interest being infringed and that are occurring concurrently, committed by the same operator, in at least three Member States;

(44f) 'widespread infringement with a Union dimension' means a widespread infringement that has harmed or is likely to harm the collective interests of individuals in at least two-thirds of the Member States, accounting, together, for at least two-thirds of the population of the Union.

(44h) 'regulatory sandbox' means a controlled environment established by a public authority that facilitates the safe development, testing and validation of innovative AI systems for a limited time before their placement on the market or putting into service pursuant to a specific plan under regulatory supervision;

(44i) 'critical infrastructure' means an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service within the meaning of Article 2(4) of Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities;

(45c) 'social scoring' means evaluating or classifying natural persons based on their social behaviour, socio-economic status or known or predicted personal or personality characteristics;

(45d) 'social behaviour' means the way a natural person interacts with and influences other natural persons or society;

(45e) 'state of the art' means the developed stage of technical capability at a given time as regards products, processes and services, based on the relevant consolidated findings of science, technology and experience;

(45f) 'testing in real world conditions' means the temporary testing of an AI system for its intended purpose in real world conditions outside of a laboratory or otherwise simulated environment;

~~*Article 4*~~
~~*Amendments to Annex I*~~

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

Article 4a
General principles applicable to all AI systems

1. All operators falling under this Regulation shall make their best efforts to develop and use AI systems or foundation models in accordance with the following general principles establishing a high-level framework that promotes a coherent human-centric European approach to ethical and trustworthy Artificial Intelligence, which is fully in line with the Charter as well as the values on which the Union is founded:

a) ***'human agency and oversight' means that AI systems shall be developed and used as a tool that serves people, respects human dignity and personal autonomy, and that is functioning in a way that can be appropriately controlled and overseen by humans.***
b) ***'technical robustness and safety' means that AI systems shall be developed and used in a way to minimize unintended and unexpected harm as well as being robust in case of unintended problems and being resilient against attempts to alter the use or performance of the AI system so as to allow unlawful use by malicious third parties.***
c) ***'privacy and data governance' means that AI systems shall be developed and used in compliance with existing privacy and data protection rules, while processing data that meets high standards in terms of quality and integrity.***
d) ***'transparency' means that AI systems shall be developed and used in a way that allows appropriate traceability and explainability, while making humans aware that they communicate or interact with an AI system as well as duly informing users of the capabilities and limitations of that AI system and affected persons about their rights.***
e) ***'diversity, non-discrimination and fairness' means that AI systems shall be developed and used in a way that includes diverse actors and promotes equal access, gender equality and cultural diversity, while avoiding discriminatory impacts and unfair biases that are prohibited by Union or national law.***
f) ***'social and environmental well-being' means that AI systems shall be developed and used in a sustainable and environmentally friendly manner as well as in a way to benefit all human beings, while monitoring and assessing the long-term impacts on the individual, society and democracy.***

2. ***Paragraph 1 is without prejudice to obligations set up by existing Union and national law. For high-risk AI systems, the general principles are translated into and complied with by providers or deployers by means of the requirements set out in Articles 8 to 15, and respective obligations laid down in Chapter 3 of Title III of this Regulation. For foundation models, the general principles are translated into and complied with by providers by means of the requirements set out in Articles 28 to 28b. For all AI systems, the application of the principles referred to in paragraph 1 can be achieved, as applicable, through the provisions of Article 28, Article 52, or the application of harmonised standards, technical specifications, and codes of conduct as referred to in Article 69,without creating new obligations under this Regulation.***

3. ***The Commission and the AI Office shall incorporate these guiding principles in standardisation requests as well as recommendations consisting in technical guidance to assist providers and deployers on how to develop and use AI systems. European Standardisation Organisations shall take the general principles referred to in paragraph 1 into account as outcome-based objectives when developing the appropriate harmonised standards for high risk AI systems as referred to in Article 40(2b).***

Article 4d
AI literacy

1. When implementing this Regulation, the Union and the Member States shall promote measures for the development of a sufficient level of AI literacy, across sectors and taking into account the different needs of groups of providers, deployers and affected persons concerned, including through education and training, skilling and reskilling programmes and while ensuring proper gender and age balance, in view of allowing a democratic control of AI systems.

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

3. Such literacy measures shall consist, in particular, of the teaching of basic notions and skills about AI systems and their functioning, including the different types of products and uses, their risks and benefits.

4. A sufficient level of AI literacy is one that contributes, as necessary, to the ability of providers and deployers to ensure compliance and enforcement of this Regulation.

~~ANNEX I~~
~~ARTIFICIAL INTELLIGENCE TECHNIQUES AND APPROACHES~~
~~referred to in Article 3, point 1~~

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

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

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