Council of the European Union

Brussels, 19 October 2022
(OR. en)

13102/22

Interinstitutional File:
2021/0106(COD)

LIMITE

TELECOM 390
JAI 1263
COPEN 338
CYBER 313
DATAPROTECT 267
EJUSTICE 77
COSI 242
IXIM 232
ENFOPOL 483
FREMP 200
RELEX 1280
MI 704
COMPET 755
CODEC 1402

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	12549/22
No. Cion doc.:	8115/21
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Fourth Presidency compromise text

I. INTRODUCTION

1. The Commission adopted the proposal for a Regulation laying down harmonised rules on artificial intelligence **(Artificial Intelligence Act, AIA)** on 21 April 2021.

Obtenu pour vous par
Got for you by
agence europe

2. The Slovenian Presidency drafted the first, partial compromise proposal, which covered **Articles 1-7 and Annexes I-III** of the proposed AIA. The French Presidency continued the drafting process and by the end of its term it redrafted the remaining parts of the text **(Articles 8-85 and Annexes IV-IX)** and presented the entire first consolidated compromise proposal on the AIA on 17 June 2022.

3. On 5 July 2022, the Czech Presidency held a policy debate in WP TELECOM on the basis of a policy options paper, the outcomes of which were used to prepare **the second compromise text.** Based on the reactions of the delegations to this compromise, the Czech Presidency prepared **the third compromise text**, which was presented and discussed in WP TELECOM on 22 and 29 September 2022. After these discussions, the delegations were asked to send in their written comments on the points they felt most strongly about. Based on those comments, as well as using the input obtained during bilateral contacts with the Member States, the Czech Presidency has now drafted **the fourth compromise proposal**, which can be found in the Annex.

4. **During the WP TELECOM meeting on 25 October 2022, the Czech Presidency intends to present the changes made in the fourth compromise proposal, and invites the delegations to indicate any outstanding issues with the text.**

5. The changes in the document compared with the third compromise text issued by the Czech Presidency (doc. 12549/22) are underlined. Compared with the Commission's proposal, additions are marked with **bold**, deletions with ~~strikethrough~~.

Obtenu pour vous par
Got for you by
agence europe

II. MAIN CHANGES

1. Title I - General provisions

1.1 In **Article 2(3)** the reference to the use of AI systems has been added in order to align it with **Article 1(a)**. Moreover, **Article 2(3a)** has been deleted, because the exclusion of use from the scope has been included in **Article 2(3)**. In the second subparagraph of **Article 2(3)** the last sentence has been added to ensure alignment with the first subparagraph, and corresponding modifications have also been made in **Recital (-12a).**

1.2 A new **Article 2(8)** has been added to clarify that the AI Act does not apply to the obligations of private non-professional users who are natural persons, with the exception of transparency obligations laid down in **Article 52**.

1.3 In **Article 3(1)**, the reference to 'a certain level' of autonomy has been replaced with 'elements' of autonomy for reasons of clarity and precision.

1.4 The definition of 'common specifications' in **Article 2(28)** has been updated to align it with the horizontal approach used in relation to the proposal for a Regulation on Machinery Products.

1.5 In the definition of 'emotional recognition systems' in **Article 3(34)** a reference to 'psychological states' has been added to make the definition more complete and future proof.

Obtenu pour vous par
Got for you by
agence europe

1.6 In **Article 3(36)** the words 'remote' and 'at a distance' have been reinstated to bring back the original wording of the term 'remote biometric identification'. This was done in order to eliminate doubts about the possible inclusion of systems used for identification, which should not be covered by this definition, including for instance the fingerprint identification systems. A further clarification has been made that remote biometric identification happens without active involvement of persons, and for this reason the examples of systems that would not be covered by this definition have been deleted from the second part of the definition. Consequently, the word 'remote' has been reinstated in all instances where it was previously deleted, notably in **Article 5** and in **Annex III**. **Recital (8)** that clarifies the notion of remote biometric identification has also been updated accordingly.

1.7 The changes in the definition of 'national competent authority' in **Article 3(43)** are meant to clarify that for AI systems put into service or used by EU institutions, it is the EPDS that should fulfil the responsibilities that in the Member States are entrusted to national competent authorities. Consequently, with this clarification it is no longer necessary to make this explicit in every instance where national competent authorities or market surveillance authorities are mentioned, and the entire text of the AI Act has been updated accordingly by removing references to the EDPS (e.g. deletion of **Article 53(-1b)**, deletions in **Articles 54a(4) and 54a(7)**, deletion in **Article 63a(2)** and in many other instances throughout the text). **Recital (79)** also further clarifies that this is without prejudice to the designation of national competent authorities by the Member States.

2. Title I_A - General purpose AI systems

2.1 In **Article 4a(1)** references to Articles 53 and 69 have been added to clarify that general purpose AI providers can also participate in the sandboxes and apply codes of conduct.

Obtenu pour vous par
Got for you by
agence europe

2.2 In **Article 4b(1)**, specificities of the AI value chain was added as another aspect that the Commission will have to take into account when preparing the respective implementing acts. The last sentence of **Article 4b(1),** linking harmonised standards and common specifications to state of the art, has been deleted in order to align the wording with the corresponding change in **Article 8(1)**. The corresponding reference to state of the art has now been included in **Recital 61,** in line with the Commission's non-paper on horizontal approach on common specifications complementary to harmonised European standards, which was issued during the negotiations on the proposal for the Regulation on Machinery Products.

3. Title II - Prohibited artificial intelligence practices

3.1 As mentioned in point 1.6 above, the word 'remote' has been reinstated as part of the term 'remote biometric identification' throughout **Article 5**.

3.2 **Article 5(4a)** has been deleted because with the reinstatement of the word 'remote' in 'remote biometric identification' in **Article 5(1)(d)**, the non-prejudice provision that it lays down is no longer needed.

4. Title III - High-risk AI systems

4.1 In the last subparagraph of **Article 6(3)** some modifications have been made in order to better clarify the objective of the future implementing acts specifying how purely accessory nature should be understood with regard to the output of AI systems referred to in Annex III.

4.2 In **Article 13(3)(b)** **point (vi)** has been added to indicate that a description of the expected output of a high-risk AI system should also be included in the instructions for use. A corresponding change has also been made in **Annex IV**.

4.3 **Article 14(5)** has been modified in order to extend the exception from the 4-eyes principle laid down in that article also to law enforcement and immigration authorities.

Obtenu pour vous par
Got for you by
agence europe

4.4 In **Article 17** a new **paragraph 2a** has been added in order to ensure further alignment with sectoral legislation with regard to obligations related to quality management systems and with a similar provision in **Article 9(9)** as regards the risk management system.

4.5 **Article 18(2)** has been updated in line with the changes introduced in the third compromise text with regards to financial institutions (mirroring e.g. the changes in **Article 20(2)**).

4.6 In **Article 29**, the requirement for users to implement human oversight has been moved from **paragraph 1** to **paragraph 4**, where it fits better conceptually.

4.7 **Article 29(7)** has been deleted because the exemption from the obligations under the AI Act for private non-professional users who are natural persons has now been included in the new **Article 2(8)**, as indicated in in point 1.2 above.

4.8 **Article 41** on common specifications contains several modifications, which have been introduced to ensure consistency with the Commission's non-paper on horizontal approach on common specifications complementary to harmonised European standards, which was issued during the negotiations on the proposal for the Regulation on Machinery Products. Corresponding clarifications have also been made in **Recital 61**.

4.9 **Article 51(1)** has been modified in order to provide an exemption from the requirement to register in the EU database certain high-risk AI systems (and their providers) referred to in Annex III in the areas of law enforcement, migration, asylum and border control management, as well as critical infrastructure. Similarly, **Article 51(2)** has been updated to indicate that users of high-risk AI systems in the area of critical infrastructure that are public authorities, agencies or bodies will also be exempted from the obligation to register in the EU database for high-risk AI systems. **Recital 69** that provides further explanations on this subject has been updated accordingly.

Obtenu pour vous par
Got for you by
agence europe

5. Title IV - Transparency obligations for providers and users of certain AI systems

5.1 In **Article 52(3)** it has been clarified that transparency obligations laid down in this article should not impede the right to freedom of the arts, in particular where the content is part of an evidently creative, satirical, artistic or fictional work or programme. Additional clarifications in this respect have also been made in **Recital 70**.

6. Title V- Measures in support of innovation

6.1 In **Article 53(1b)** evidence-based regulatory learning has been included as an additional objective of the establishment of AI regulatory sandboxes.

6.2 In **Article 53(4a), first subparagraph,** 'may' has been changed into 'shall' to make the issuance of exit reports obligatory for national competent authorities. In the **second subparagraph** it has been clarified that the Commission and the AI Board should use the learning outcomes from AI sandboxes when exercising their tasks under the AI Act and that there should be a possibility to make the exit reports publicly available, subject to agreement of concerned parties.

6.3 An additional subparagraph has been added in **Article 53(6)** to provide for more flexibility in the future implementing acts for national competent authorities to establish and operate AI regulatory sandboxes.

6.4 **Article 54a(4)(c)** has been updated in order to align it with the changes in **Article 51**, and it provides for exemptions from the obligation to register the testing in real world conditions in the EU database, when it is related to certain high-risk AI systems referred to in Annex III in the areas of law enforcement, migration, asylum and border control management, as well as critical infrastructure.

Obtenu pour vous par
Got for you by
agence europe

7. Title VI - Governance

7.1 **Article 58(h)** has been modified to indicate that the AI Board should assist the work of market surveillance authorities and support cross-border market surveillance investigations, in particular as regards the emergence of risks of systemic nature that may stem from AI systems.

8. Title VIII - Post-market monitoring, information sharing, market surveillance

8.1 The modifications in **Articles 63(4), second subparagraph,** are meant to provide the Member States with the discretion to designate authorities different from the 'relevant national authority responsible for financial supervision' as the market surveillance authority for financial institutions for the purpose of the AI Act, if this is done in justified circumstances and deemed more appropriate by the relevant Member State.

8.2 The addition at the end of **Article 63(5)** is meant to ensure that market surveillance activities will not impact the independence of courts.

8.3 In **Article 68b(1)** 'may' has been replaced with 'shall' in order to make it obligatory for the Commission, upon the request of the AI Board, to adopt an implementing act providing for the creation of a central pool of independent experts

9. Title X - Confidentiality and penalties

9.1 In **Article 71(4)** two more points have been added to complete the list of provisions the infringements of which should be subject to fines laid down in this paragraph and to correct the omissions in the third compromise text. **Point (-a)** covers infringements of provisions concerning providers of general purpose AI systems and **point (h)** covers infringements of transparency obligations.

Obtenu pour vous par
Got for you by
agence europe

9.2 In **Article 71(6)** four more points have been added to further safeguard the proportionality of the fines. These additional principles are based on similar provisions in Article 83 of the GDPR

10. Title XII – Final provisions

10.1 **Article 83(3)** was deleted as it was not considered to be essential.

11. Annex III - High-risk AI systems referred to in Article 6(3)

11.1 In **point 1(a)** the word 'remote' has been reinstated, as described in point 1.6 above.

11.2 In **point 2** letter (aa) has been merged with letter (a).

11.3 In **point 5** letter (e) has been added in order to reinsert some specific use cases from the area of insurance to the list of areas in which the use of AI systems is considered to be high-risk.

12. Annex IV

12.1 In **point 2(b)** the requirement to include the description of the expected output of the AI system in technical documentation has been added**.**

13. Annex VIII

13.1 **Points (4) and (10) of Part II** have been modified to reflect the fact that there is now a full exemption in **Article 51** from the obligation to register in the EU database high-risk AI systems in the areas of law enforcement and migration, asylum and border control management.

Obtenu pour vous par
Got for you by
agence europe

14. Other changes

14.1 **Recital 6** has been slightly modified, with the addition of examples of some key functional characteristics of AI (learning, reasoning or modelling capabilities) and clarification of the fact that final objectives of AI systems are given by humans, while intermediary objectives could also be set by these systems without human intervention.

14.2 **Recitals 34, 35 and 37** have been updated to ensure their consistency with the revised **Annex III**. Moreover, **Recital 34** now includes some examples of safety components of critical infrastructure.

14.3 The addition at the end of **Recital 38** is meant to clarify that AI systems specifically intended to be used by financial intelligence units with administrative tasks should not be considered as high-risk AI systems.

14.4 **Recital 58** contains a clarification that user obligations under the AI Act should be without prejudice to other user obligations in relation to high-risk AI systems under Union or national law.

14.5 The first sentence of **Recital 58a** has been moved to **Recital 5a** and slightly adapted.

14.6 The addition at the end of **Recital 63** is meant to take into account the specific requirement for benefit-risk assessment that only applies to the Medical Devices Regulation and the In Vitro Diagnostic Medical Devices Regulation.

14.7 **Recital 72a** has been updated in order to ensure consistency with the law enforcement exception as regards consent to participate in testing in real world conditions, as provided for in **Article 54**, and to clarify the difference between consent to participate in testing in real world conditions and consent under the GDPR.

Obtenu pour vous par
Got for you by
agence europe

14.8 In **Recital 76** a modification has been introduced to indicate that the Commission should be obliged to support the activities of the standing subgroup for market surveillance, including by undertaking relevant market evaluations or studies. It also further specifies that a cooperation with relevant actors active in the context of other EU regulation on digital products and services should be ensured.

14.9 In addition to the changes listed above, some further minor clarifications and corrections have been made in **Articles 9, 37, 58(c), 59, 60** as well in **Recitals 5, 6a, 12b, 36, 47, 79, 80, 83 and 86.**

_____

Obtenu pour vous par
Got for you by
agence europe

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,

Having regard to the proposal from the European Commission,

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

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

Having regard to the opinion of the Committee of the Regions[2],

Having regard to the opinion of the European Central Bank[3],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The purpose of this Regulation is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, marketing and use of artificial intelligence in conformity with Union values. This Regulation pursues a number of overriding reasons of public interest, such as a high level of protection of health, safety and fundamental rights, and it 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.

[1] OJ C […], […], p. […].
[2] OJ C […], […], p. […].
[3] Reference to ECB opinion

Obtenu pour vous par
Got for you by
agence europe

(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 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**, import** or use AI systems. A consistent and high level of protection throughout the Union should therefore be ensured, while divergences hampering the free circulation 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). To the extent that this Regulation contains specific rules on the protection of individuals with regard to the processing of personal data concerning restrictions of the use of AI systems for 'real-time' ~~remote~~ **remote** biometric identification in publicly accessible spaces for the purpose of law enforcement, it is appropriate to base this Regulation, in as far as those specific rules are concerned, on Article 16 of the TFEU. In light of those specific rules and the recourse to Article 16 TFEU, it is appropriate to consult the European Data Protection Board.

(3) Artificial intelligence is a fast evolving family of technologies that can contribute to a wide array of economic and societal benefits across the entire spectrum of industries and social activities. By improving prediction, optimising operations and resource allocation, and 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, education and training, infrastructure management, energy, transport and logistics, public services, security, justice, resource and energy efficiency, and climate change mitigation and adaptation.

(4) At the same time, depending on the circumstances regarding its specific application and use, artificial intelligence may generate risks and cause harm to public interests and rights that are protected by Union law. Such harm might be material or immaterial.

(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 and the protection of fundamental rights, as recognised and protected by Union law. To achieve that objective, rules regulating the placing on the market and putting into service 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. By laying down those rules **and building on the work of the High-level Expert Group on Artificial Intelligence as reflecetd in the Guidelines for Trustworthy Artificial Intelligence in the EU**, this Regulation supports the objective 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].

---

[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).

Obtenu pour vous par
Got for you by
agence europe

(5a) **The harmonised rules on the placing on the market, putting into service and use of AI systems laid down in this Regulation should apply across sectors and, in line with its New Legislative Framework approach, should be without prejudice to existing Union law, ~~and in particular without prejudice to Union law~~ notably on data protection, consumer protection, fundamental rights, ~~product safety and~~ employment and product safety, to which this Regulation is complementary. As a consequence all rights and remedies afforded by such Union law to consumers and other persons who may be negatively impacted by AI systems, including as regards the compensation of possible damages pursuant to Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, remain unaffected and fully applicable. On top of that, t~~T~~his Regulation aims to strengthen the effectiveness of such existing rights and remedies by establishing specific requirements and obligations, including in respect of transparency, technical documentation and record-keeping of AI systems ~~is intended to regulate AI systems that are to be placed on the market and put into service in the Union and it should complement such existing Union law~~. Furthermore, the obligations placed on various operators involved in the AI value chain under this Regulation should apply without prejudice to national laws, in compliance with Union law, having the effect of limiting the use of certain AI systems where such laws fall outside the scope of this Regulation or pursue other legitimate public interest objectives than those pursued by this Regulation. For example, national labour law and the laws on the protection of minors (i.e. persons below the age of 18) taking into account the United Nations General Comment No 25 (2021) on children's rights, insofar as they are not specific to AI systems and pursue other legimitate public interest objectives, should not be affected by this Regulation.**

(6) The notion of AI system should be clearly defined to ensure legal certainty, while providing the flexibility to accommodate future technological developments. The definition should be based on ~~the~~ key functional characteristics ~~of the software~~ **of artificial intelligence such as its learning, reasoning or modelling capabilities, distinguishing it from ~~more classic~~ simpler software systems and programming approaches. ~~, i~~In** particular**, for the purposes of this Regulation AI systems should ~~be intended as~~ have~~ing~~** the ability, **on the basis of machine and/or human-based data and inputs, to infer the way to achieve a ~~given~~ set of ~~human-defined~~ final objectives given to them by humans, using machine learning and/or logic- and knowledge based approaches ~~through learning, reasoning or modelling~~ and to** ~~for a given set of human-defined objectives, to~~ ~~generate~~ **produce ~~specific~~** outputs **~~in the form of~~** ~~such as~~ **such as** content **for generative AI systems (e.g. ~~such as~~ text, video or images)**, ~~as well as~~ predictions, recommendations~~,~~ or decisions**,** ~~which~~ influenc**ing** the environment with which the system interacts, be it in a physical or digital dimension. **A system that uses rules defined solely by natural persons to automatically execute operations should not be considered an AI system.** AI systems can be designed to operate with varying levels of autonomy and be used on a stand-alone basis or as a component of a product, irrespective of whether the system is physically integrated into the product (embedded) or serve the functionality of the product without being integrated therein (non-embedded). **The concept of the autonomy of an AI system relates to the degree to which such a system functions without ~~external influence~~ human involvement.**

(6a) **Machine learning approaches focus on the development of systems capable of learning and inferring from data to solve an application problem without being explicitly programmed with a set of step-by-step instructions from input to output. Learning refers to the computational process of optimizing from data the parameters of the**

Obtenu pour vous par
Got for you by
agence europe

model, which is a mathematical construct generating an output based on input data. The range of problems addressed by machine learning typically involves tasks for which other approaches fail, either because there is no suitable formalisation of the problem, or because the resolution of the problem is intractable with non-learning approaches. Machine learning approaches include for instance supervised, unsupervised and reinforcement learning, using a variety of methods including deep learning <u>with neural networks</u>, statistical techniques for learning and inference (including for instance logistic regression, Bayesian estimation) and search and optimisation methods.

(6b) Logic- and knowledge based approaches focus on the development of systems with logical reasoning capabilities on knowledge to solve an application problem. Such systems typically involve a knowledge base and an inference engine that generates outputs by reasoning on the knowledge base. The knowledge base, which is usually encoded by human experts, represents entities and logical relationships relevant for the application problem through formalisms based on rules, ontologies, or knowledge graphs. The inference engine acts on the knowledge base and extracts new information through operations such as sorting, searching, matching or chaining. Logic- and knowledge based approaches include for instance knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning, expert systems and search and optimisation methods.

(6c) In order to ensure uniform conditions for the implementation of this Regulation as regards machine learning approaches and logic- and knowledged based approaches and to take account of ~~The definition of AI system should be complemented by a list of specific techniques and approaches used for its development, which should be kept up-to-date in the light of~~ market and technological developments**, implementing powers should be conferred on the Commission.**~~through the adoption of delegated acts by the Commission to amend that list.~~

(6d) The notion of 'user' referred to in this Regulation should be interpreted as any natural or legal person, including a public authority, agency or other body, using an AI system under whose authority the system is used. Depending on the type of AI system, the use of the system may affect persons other than the user.

(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[6], Article 3(18) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[7] and Article 3(13) of Directive (EU) 2016/680 of the European Parliament and of the Council[8].

---

6 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).

7 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39)

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

Obtenu pour vous par
Got for you by
agence europe

(8) The notion of ~~remote~~ **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~~ **typically at a distance, without their active involvement,** through the comparison of a person's biometric data with the biometric data contained in a reference ~~database~~ **data repository,** irrespectively of the particular technology, processes or types of biometric data used**. Such remote biometric identification systems are typically used to perceive (scan) multiple persons or their behaviour simultaneously in order to facilitate significantly the identification of a number of persons without their active involvement. Such a definition excludes verification/authentification systems whose sole purpose would be to confirm that a specific natural person is the person he or she claims to be, as well as systems that are used to confirm the identity of a natural person for the sole purpose of having access to a service, a device or premises. This exclusion is justified by the fact that such systems are likely to have a minor impact on fundamental rights of natural persons compared to remote biometric identification systems which may be used for the processing of the biometric data of a large number of persons.** ~~**and without prior knowledge whether the targeted person will be present and can be identified**~~. ~~**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.

(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 **an undetermined number of natural persons** ~~the public~~, **and irrespective of whether the place in question is privately or publicly owned. and irrepective of the activity for which the place may be used, such as commerce (for instance, shops, restaurants, cafés), services (for instance, banks, professional activities, hospitality), sport (for instance, swimming pools, gyms, stadiums), transport (for instance, bus, metro and railway stations, airports, means of transport), entertainment (for instance, cinemas, theatres, museums, concert and conference halls) leisure or otherwise (for instance, public roads and squares, parks, forests, playgrounds). A place should be classified as publicly accessible also if, regardless of potential capacity or security restrictions, access is subject to certain predetermined conditions, which can be fulfilled by an undetermined number of persons, such as purchase of a ticket or title of transport, prior registration or having a certain age. By contrast, a place should not be considered publicly accessible if access is limited to specific and defined natural persons through either Union or national law directly related to public safety or security or through the clear manifestation of will by the person having the relevant authority on the place. The factual possibility of access alone (e.g. an unlocked door, an open gate in a fence) does not imply that the place is publicly accessible in the presence of indications or circumstances suggesting the contrary (e.g. signs prohibiting or restricting access). Company and factory premises as well as offices and workplaces that are intended to be accessed only by relevant**

Obtenu pour vous par
Got for you by
agence europe

employees and service providers are places that are not publicly accessible. Publicly accessible spaces should not include prisons or border control areas. Some other areas may be composed of both not publicly accessible and publicly accessible areas, such as the hallway of a private residential building necessary to access a doctor's office or an airport. ~~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, 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.

(10) In order to ensure a level playing field and an effective protection of rights and freedoms of individuals across the Union, the rules established by this Regulation should apply to providers of AI systems in a non-discriminatory manner, irrespective of whether they are established within the Union or in a third country, and to users of AI systems established within 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 of AI systems that are established in a third country, to the extent the output produced by those systems is used in the Union. Nonetheless, to take into account existing arrangements and special needs for **future** cooperation with foreign partners with whom information and evidence is exchanged, this Regulation should not apply to public authorities of a third country and international organisations when acting in the framework of 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. **Recipient Member States authorities and Union institutions, offices, bodies and bodies making use of such outputs in the Union remain accountable to ensure their use comply with Union law. When those international agreements are revised or new ones are concluded in the future, the contracting parties should undertake the utmost effort to align those agreements with the requirements of this Regulation.**

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

Obtenu pour vous par
Got for you by
agence europe

(-12a) **If and insofar** AI systems **are** ~~[exclusively]developed~~ **placed on the market, ~~or~~ put into service, or used with or without modification of such systems** ~~or used~~ for military, ~~**or**~~ **defence or national security** purposes**, those** should be excluded from the scope of this Regulation **regardless of which type of entity is carrying out those activities, such as whether it is a public or private entity**. **As regards military and defence purposes, ~~S~~such exclusion is justified both by Article 4(2) TEU and by the specifities of the Member States' and the common Union defence policy covered by Chapter 2 of Title V of the Treaty on European Union (TEU) that are subject to public international law, which is therefore the more appropriate legal framework for the regulation of AI systems in the context of the use of lethal force and other AI systems in the context of military and defence activities. As regards national security purposes, the exclusion is justified both by the fact that national security remains the sole responsibility of Member States in accordance with Article 4(2) TEU and by the specific nature and operational needs of national security activities and specific national rules applicable to those activities. Nonetheless, if an AI system ~~developed placed on the market or put into service exclusively~~ developed, placed on the market, ~~or~~ put into service or used ~~exclusively~~ for military, ~~or~~ defence or national security purposes is used ~~outside those~~ outside those temporarily or permanently for other purposes (for example, civilian or humanitarian purposes, law enforcement or public security purposes), such a system would fall within the scope of this Regulation. In that case, the entity using the system for other than military, ~~or~~ defence or national security purposes should ensure compliance of the system with this Regulation, unless the system is already compliant with this Regulation. AI systems placed on the market or put into service for an excluded ~~both~~ (i.e. military, ~~or~~ defence or national security) and one or more non excluded purposes (e.g. ~~and~~ civilian purposes, law enforcement, etc.), fall within the scope of this Regulation and providers of those systems should ensure compliance with 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).~~ ~~**If and insofar When AI systems are exclusively developed placed on the market or put into service or used for national security purposes, they should also be excluded from the scope of the Regulation, regardless of which type of entity is carrying out those activities, such as whether it is a public or private entity. taking into account Such exclusion is justified both by the fact that national security remains the sole responsibility of Member States in accordance with Article 4(2) TEU and by the specific nature and operational needs of national security activities and specific national rules applicable to those activities. Nonetheless, if an AI system placed on the market or put into service for national security purposes is used outside those purposes (for example, for safeguarding public security or for law enforcement), such a system would fall within the scope of this Regulation. In that case, the entity using the system for other than national security purposes should ensure compliance of the system with this Regulation, unless the system is already compliant with this Regulation. AI systems placed on the market or put into service for both national security and other purposes, including law enforcement, fall within the scope of this Regulation and providers of those systems should ensure compliance. In those cases, t**~~ **In those cases, ~~T~~the fact that an AI system may fall within the scope of this Regulation should not affect the possibility of entities carrying out ~~the~~ national security, ~~and~~ defence and military activities, regardless of the type of entity carrying out those activities, ~~agencies and entities acting on their behalf~~ to use ~~that~~ AI systems for national security, military and defence purposes~~.~~, ~~which fall outside~~ the use of which is excluded from the scope of this Regulation. ~~For example, regardless of whether a~~An AI system placed on the market**

Obtenu pour vous par
Got for you by
agence europe

for civilian or law enforcement purposes which is used with or without modification for ~~specific~~ military, defence or national security purposes ~~, that system~~ should not fall within the scope of this Regulation, regardless of the type of entity carrying out those activities. ~~insofar as military, defence or national security purposes are concerned~~.

(12a) 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].

(12b) This Regulation should not undermine research and development activity and should respect freedom of science. It is therefore necessary to exclude from its scope AI systems specifically developed and put into service 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. As regards product oriented research activity by providers, the provisions of this Regulation should also not apply. This is without prejudice to the obligation to comply with this Regulation when an AI system falling into the scope of this Regulation is placed on the market or put into service as a result of such research and development activity and to the application of provisions on regulatory sandboxes and testing in real world conditions~~insofar as such research leads to or entails placing an AI system on the market or putting it into service~~. Furthermore, without prejudice to the foregoing regarding AI systems specifically developed and put into service for the sole purpose of scientific research and development, any other AI system that may be used for the conduct of any reaserch and development activity should remain subject to the provisions of this Regulation. Under all circumstances, any research and development activity should be carried out in accordance with recognised ethical and professional standards for scientific research.

(12c) In the light of the nature and complexity of the value chain for AI systems, it is essential to clarify the role of actors who may contribute to the development of AI systems, notably high-risk AI systems. In particular, it is necessary to clarify that general purpose AI systems are AI systems that are intended by the provider to perform generally applicable functions, such as image/speech recognition, and in a plurality of contexts. They may be used as high-risk AI systems by themselves or be components of other high risk AI systems. Therefore, due to their ~~peculiar~~ particular nature and in order to ensure a fair sharing of responsibilities along the AI value chain, such systems should be subject to proportionate and ~~tailored~~ more specific requirements and obligations under this Regulation, ~~before their placing on the Union market or putting into service,~~ while ensuring a high level of protection of fundamental rights, health and safety. ~~Therefore~~ In addition, the providers of general purpose AI systems, irrespective of whether they may be used as high-risk AI systems as such by other providers or as components of high-risk AI systems, should cooperate, as appropriate, with the ~~final~~ providers of the respective high-risk AI systems to enable their compliance with the relevant obligations under this Regulation and with the competent authorities established under this Regulation. In order to take into account the specific characteristics of general purpose AI systems and the fast evolving market and technological developments in the field, implementing powers should be conferred on the Commission to specify and adapt the application of the requirements established under this Regulation to general purpose AI systems and to specify the information to be shared by the providers of general purpose AI systems in order to enable the providers of the respective high-risk AI system to comply with their obligations under this Regulation.

Obtenu pour vous par
Got for you by
agence europe

(13) In order to ensure a consistent and high level of protection of public interests as regards health, safety and fundamental rights, 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) and should be non-discriminatory and in line with the Union's international trade commitments.

(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 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 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) **AI-enabled manipulative techniques can be used to persuade persons to engage in unwanted behaviours, or to deceive them by nudging them into decisions in a way that subverts and impairs their autonomy, decision-making and free choices.** The placing on the market, putting into service or use of certain AI systems ~~intended to distort~~ **materially distorting** human behaviour, whereby physical or psychological harms are likely to occur, **are particularly dangerous** and should **therefore** be forbidden. Such AI systems deploy subliminal components **such as audio, image, video stimuli** ~~individuals~~ **that persons** cannot perceive **as those stimuli are beyond human perception or other subliminal techniques that subvert or impair person's autonomy, decision-making or free choices in ways that people are not consciously aware of, or even if aware not able to control or resist, for example in cases of machine-brain interfaces or virtual reality. In addition, AI systems may also** ~~or those sysems~~ **otherwise** exploit vulnerabilities of ~~children and people~~ **a specific group of persons** due to their age, ~~physical or mental incapacities. They do so with the intention to materially distort~~ **disability within the meaning of Directive (EU) 2019/882, or a specific social or economic situation that is likely to make those persons more vulnerable to exploitation such as persons living in extreme poverty, ethnic or religious minorities. Such AI systems can be placed on the market, put into service or used with the objective to or the effect of materially distorting** the behaviour of a person and in a manner that causes or is **reasonably** likely to cause **physical or phycological** harm to that or another person~~. The intention~~ **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 ~~of human behaviour~~ results from factors external to the AI system which are outside of the control of the provider or the user~~. Research for legitimate purposes in relation to such AI systems should~~, **meaning factors that may** not be ~~stifled~~ **reasonably foreseen and mitigated** by the ~~prohibition, if such research does not amount to use~~ **provider or the user** of the AI system~~ in human-machine relations that exposes natural persons to~~ **. In any case, it is not necessary for the provider or the user to have the intention to cause the physical or psychological** harm ~~and such research is carried out in accordance with recognised ethical standards~~**, as long as such harm results from the manipulative or exploitative AI-enabled practices. The prohibitions** for ~~scientific research~~ **such AI practices are** ~~is~~ **complementary to the provisions contained in Directive** ~~[Unfair Commercial Practice Directive~~ **2005/29/EC**~~, as amended by Directive~~

Obtenu pour vous par
Got for you by
agence europe

~~(EU) 2019/216]~~**, notably that unfair commercial practices leading to economic or financial harms to consumers are prohibited under all circumstances, irrespective of whether they are put in place through AI systems or otherwise**. **The prohibitions of manipulative and exploitative practices in this Regulation should not affect lawful practices in the context of medical treatment such as psychological treatment of a mental disease or physical rehabilitation, when those practices are carried out in accordance with the applicable medical standards and legislation. In addition, common and legitimate commercial practices that are in compliance with the applicable law should not in themselves be regarded as constituting harmful manipulative AI practices.**

(17) AI systems providing social scoring of natural persons ~~for general purpose~~ by public authorities or **by private actors** ~~on their behalf~~ may lead to discriminatory outcomes and the exclusion of certain groups. They may violate the right to dignity and non-discrimination and the values of equality and justice. Such AI systems evaluate or classify ~~the trustworthiness of~~ natural persons based on their social behaviour in multiple contexts or known 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 **entailing such unacceptable scoring practices** should be therefore prohibited. **This prohibition should not affect lawful evaluation practices of natural persons done for one or more specific purpose in compliance with the law**.

(18) The use of AI systems for 'real-time' ~~remote~~ **remote** biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement is considered particularly intrusive in the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights. 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.

(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[9] 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~~ **remote** biometric identification systems. Moreover, of the 32 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~~ **remote** biometric identification will

[9] 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).

Obtenu pour vous par
Got for you by
agence europe

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. **In addition, this Regulation should preserve the ability for law enforcement, border control, immigration or asylum authorities to carry out identity checks in the presence of the person that is concerned~~,~~ in accordance with the conditions set ~~up~~ out in Union and national law for such checks. In particular, law enforcement, border control, immigration or asylum authorities should be able to use information systems, in accordance with Union or national law, to identify a person who, during an identity check, either refuses to be identified or is unable to state or prove his or her identity, without being required by this Regulation to obtain prior authorisation. This could be, for example, a person involved in a crime, being unwilling, or unable due to an accident or a medical condition, to disclose their identity to law enforcement authorities.**

(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~~ **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~~ **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 **of the system with a view to identify a person or persons.**~~,~~ ~~except~~ **Exceptions to this rule should be allowed in** ~~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~~ **remote** biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement necessarily

Obtenu pour vous par
Got for you by
agence europe

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~~ **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~~ **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.~~ **For purposes other than law enforcement, Article 9(1) of Regulation (EU) 2016/679 and Article 10(1) of Regulation (EU) 2018/1725 prohibit the processing of biometric data for the purpose of uniquely identifying a natural person, unless one of the situations in the respective second paragraphs of those two articles applies.**

(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) **and (4)** 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) **and (4)** 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.

(27) High-risk AI systems should only be placed on the Union market or put into service 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. AI systems identified as high-risk should be limited to those that

Obtenu pour vous par
Got for you by
agence europe

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.

(28) AI systems could produce adverse outcomes to health and safety of persons, in particular when such systems operate as 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 performs their functions in complex environments. Similarly, in the health sector where the stakes for life and health are particularly high, increasingly sophisticated diagnostics systems and systems supporting human decisions should be reliable and accurate. 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, consumer protection, workers' rights, rights of persons with disabilities, 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.

(29) As regards high-risk AI systems that are safety components of products or systems, or which are themselves products or systems falling within the scope of Regulation (EC) No 300/2008 of the European Parliament and of the Council[10], Regulation (EU) No 167/2013 of the European Parliament and of the Council[11], Regulation (EU) No 168/2013 of the European Parliament and of the Council[12], Directive 2014/90/EU of the European Parliament and of the Council[13], Directive (EU) 2016/797 of the European Parliament and of the Council[14], Regulation (EU) 2018/858 of the European Parliament and of the Council[15], Regulation

---

10 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).

11 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).

12 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).

13 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).

14 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).

15 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).

Obtenu pour vous par
Got for you by
agence europe

(EU) 2018/1139 of the European Parliament and of the Council[16], and Regulation (EU) 2019/2144 of the European Parliament and of the Council[17], it is appropriate to amend those acts to ensure that the Commission takes into account, on the basis of the technical and regulatory specificities of each sector, and without interfering with existing governance, conformity assessment and enforcement mechanisms and authorities established therein, the mandatory requirements for high-risk AI systems laid down in this Regulation when adopting any relevant 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, it is appropriate to classify them as high-risk under this Regulation if the product in question undergoes the conformity assessment procedure with a third-party conformity assessment body pursuant to that relevant Union harmonisation legislation. In particular, such products are machinery, toys, lifts, equipment and protective systems intended for use in potentially explosive atmospheres, radio equipment, pressure equipment, recreational craft equipment, cableway installations, appliances burning gaseous fuels, medical devices, 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[18] and Regulation (EU) 2017/746 of the European Parliament and of the Council[19], 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, it is appropriate to classify them as high-risk if, in the light of their intended purpose, they pose a high risk of harm to the health and safety or the fundamental rights of persons, taking into account both the severity of the possible harm and its probability of occurrence, and they are used in a number of specifically pre-defined areas specified in the Regulation. The identification of those systems is based on the same methodology and criteria envisaged also for any future amendments of the list of high-risk AI systems. ~~**On top of that,**~~ **It is also important to**

---

16 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).

17 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).

18 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).

19 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).

Obtenu pour vous par
Got for you by
agence europe

clarify that within the high-risk scenarios referred to in Annex III there may be systems that do not lead to a significant risk to the legal interests protected under those scenarios, taking into account the output produced by the AI system. Therefore only when such output has a high degree of importance (i.e. is not purely accessory) in respect of the relevant action or decision so as to generate a significant risk to the legal interests protected, the AI system generating such output should be considered as high-risk. For instance, when the information provided by an AI systems to the human consists of the profiling of natural persons within the meaning of of Article 4(4) Regulation (EU) 2016/679 and Article 3(4) of Directive (EU) 2016/680 and Article 3(5) of Regulation (EU) 2018/1725, such information should not typically be considered of accessory nature in the context of high risk AI systems as referred to in Annex III. However, if the output of the AI system has only negligible or minor relevance for human action or decision, it may be considered purely accessory, including for example, AI systems used for translation for informative purposes or for the management of documents. ~~the significance of the ouput of the AI system in relation to the decision or action taken by a human, as well as the immediacy of the effect should also be taken into account when classifying AI systems as high risk.~~

(33) Technical inaccuracies of AI systems intended for the ~~remote~~ **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, **race,** sex or disabilities. Therefore, 'real-time' and 'post' ~~remote~~ **remote** biometric identification systems should be classified as high-risk. In view of the risks that they pose, both types of ~~remote~~ **remote** biometric identification systems should be subject to specific requirements on logging capabilities and human oversight.

(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 **critical digital infrastructure as listed in Annex I point 8 of the Directive on the resilience of critical entities,** road traffic and the supply of water, gas, heating and electricity, since their failure or malfunctioning may put at risk the life and health of persons at large scale and lead to appreciable disruptions in the ordinary conduct of social and economic activities. ~~**Considering the increasing digitalisation of all sectors of the economic and public life, it is also appropriate to classify as high risk AI systems intended to be used to control or as safety components of critical digital infrastructure as listed in Annex I point 8 of the Directive on the resilience of critical entities. Furthermore, AI systems that control emissions and pollution should also be classified as high-risk, taking into account the serious incidents and the irreversible damage to the environment and health that can be caused.**~~ **Examples of safety components of such critical infrastructure may include systems for monitoring water pressure, radiation controlling systems in relation to communication antennas or fire alarm controlling systems in cloud computing centres.**

(35) AI systems used in education or vocational training, notably for determining access**, admission** or assigning persons to educational and vocational training institutions **or programmes at all levels** or to evaluate **learning outcomes of** persons ~~on tests as part of or as a precondition for their education~~ should be considered high-risk, 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 may violate the right to education and training as well as the right not to be discriminated against and perpetuate historical patterns of discrimination.

Obtenu pour vous par
Got for you by
agence europe

(36) AI systems used in employment, workers management and access to self-employment, notably for the recruitment and selection of persons, for making decisions on promotion and termination and for task allocation **based on individual behavior or personal traits or characteristics**, 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 and livelihoods of these persons. Relevant work-related contractual relationships should involve employees and persons providing services through platforms as referred to in the Commission Work Programme 2021. Such persons should in principle not be considered users within the meaning of this Regulation. 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 impact their rights to data protection and privacy.

(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 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, disabilities, age, sexual orientation, or create new forms of discriminatory impacts. Considering the very limited scale of the impact and the available alternatives on the market, it is appropriate to exempt AI systems for the purpose of creditworthiness assessment and credit scoring when put into service by ~~small-scale providers~~ **~~SMEs,~~ micro or small entreprises, as defined in the Annex of Commission Recommendation 2003/361/EC ~~including start-ups,~~** for their own use. Natural persons applying for or receiving **essential** public assistance benefits and services from public authorities 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. 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 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. ~~**AI systems are also increasingly used in insurance for premium setting, underwriting and claims assessment which, if not duly designed, developed and used, can lead to serious consequences for people's life, including financial exclusion and discrimination.**~~ **AI systems are also increasingly used for risk assessment and pricing in the case of insurance products that include life and health insurance which, if not duly designed, developed and used, can lead to serious consequences for people's life and health, including financial exclusion and discrimination.**

Obtenu pour vous par
Got for you by
agence europe

(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 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 law enforcement authorities for individual risk assessments, polygraphs and similar tools or to detect the emotional state of natural person, ~~to detect 'deep fakes'~~, for the evaluation of the reliability of evidence in criminal proceedings, for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons, or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups, 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 **as well as by financial intelligence units carrying out adminstrative tasks analysing information pursuant to Union anti-money laundering legislation** should not be considered high-risk AI systems used by law enforcement authorities for the purposes of prevention, detection, investigation and prosecution of criminal offences.

(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 the competent public authorities charged with tasks in the fields of migration, asylum and border control management as polygraphs and similar tools or to detect the emotional state of a natural person; 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 of applications for asylum, visa and residence permits and associated complaints with regard to the objective to establish the eligibility of the natural persons applying for a status. 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

Obtenu pour vous par
Got for you by
agence europe

Parliament and of the Council[20], the Regulation (EC) No 810/2009 of the European Parliament and of the Council[21] and other relevant legislation.

(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 assist judicial authorities in ~~researching and~~ interpreting facts and the law and in applying the law to a concrete set of facts. 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~~.

(41) The fact that an AI system is classified as high risk under this Regulation should not be interpreted as indicating that the use of the system is ~~necessarily~~ lawful under other acts of Union law or under national law compatible with Union law, such as on the protection of personal data, on the use of polygraphs and similar tools or other systems to detect the emotional state of natural persons. Any such use should continue to occur solely in accordance with the applicable requirements resulting from the Charter and from the applicable acts of secondary Union law and national law. This Regulation should not be understood as providing for the legal ground for processing of personal data, including special categories of personal data, where relevant**, unless it is specifically provided for otherwise in this Regulation**.

(42) To mitigate the risks from high-risk AI systems placed or otherwise put into service on the Union market ~~for users and affected persons~~, certain mandatory requirements should apply, taking into account the intended purpose of the use of the system and according to the risk management system to be established by the provider. **In particular, the risk management system should consist of a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system. This process should ensure that the provider identifies and analyses the risks to the health, safety and fundamental rights of the persons who may be affected by the system in light of its intended purpose, including the possible risks arising from the interaction between the AI system and the environment within which it operates, and accordingly adopts suitable risk management measures <u>in the light of state of the art</u>**.

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

(44) High data quality is essential for 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 the source of

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

[21] Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) (OJ L 243, 15.9.2009, p. 1).

Obtenu pour vous par
Got for you by
agence europe

discrimination prohibited by Union law. High quality training, validation and testing data sets require the implementation of appropriate data governance and management practices. Training, validation and testing data sets should be sufficiently relevant, representative and ~~free of errors and complete 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 on which the high-risk AI system is intended to be used. **These datasets should also be as free of errors and complete as possible in view of the intended purpose of the AI system, taking into account, in a proportionate manner, technical feasibility and state of the art, the availability of data and the implementation of appropriate risk management measures so that possible shortcomings of the datasets are duly addressed. The requirement for the datasets to be complete and free of errors should not affect the use of privacy-preserving techniques in the context of the the development and testing of AI systems.** ~~In particular,~~ ~~t~~Training, validation and testing data sets should take into account, to the extent required ~~in the light of~~ **by** their intended purpose, the features, characteristics or elements that are particular to the specific geographical, 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 be able to process also special categories of personal data, as a matter of substantial public interest **within the meaning of Article 9(2)(g) of Regulation (EU) 2016/679 and Article 10(2)g) of Regulation (EU) 2018/1725**, in order to ensure the bias monitoring, detection and correction in relation to high-risk AI systems.

(44a) When applying the principles referred to in Article 5(1)(c) of Regulation 2016/679 and Article 4(1)(c) of Regulation 2018/1725, in particular the principle of data minimisation, in regard to training, validation and testing data sets under this Regulation, due regard should be had to the full life cycle of the AI system.

(45) For the development 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.

(46) Having information on how high-risk AI systems have been developed and how they perform throughout their lifecycle is essential to verify compliance with the requirements under this Regulation. 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. **Furthermore, providers or users should keep logs automatically generated by the high-risk AI system, including**

Obtenu pour vous par
Got for you by
agence europe

for instance output data, start date and time etc., to the extent that such a system and the related ~~such~~ logs are under their control, for a period that is appropriate to enable them to fulfil their obligations.

(47) To address the opacity that may make certain AI systems incomprehensible to or too complex for natural persons, a certain degree of transparency should be required for high-risk AI systems. Users should be able to interpret the system output and use it appropriately. High-risk AI systems should therefore be accompanied by relevant documentation and instructions of use and include concise and clear information, including in relation to possible risks to fundamental rights and discrimination **<u>of the persons who may be affected by the system in light of its intended purpose</u>**, where appropriate. **To facilitate the understanding of the instructions of use by users, they should contain illustrative examples, as appropriate.**

(48) High-risk AI systems should be designed and developed in such a way that natural persons can oversee their functioning. For this purpose, appropriate human oversight measures should be identified by the provider of the system before its placing on the market or putting into service. In particular, where appropriate, such measures should guarantee that the system is subject to in-built operational constraints that cannot be overridden by the system itself and is responsive to the human operator, and that the natural persons to whom human oversight has been assigned have the necessary competence, training and authority to carry out that role. **Considering the significant consequences for persons in case of incorrect matches by certain biometric identification systems, it is appropriate to provide for an enhanced human oversight requirement for those systems so that no action or decision may be taken by the user on the basis of the identification resulting from the system unless this has been separately verified and confirmed by at least two natural persons. Those persons could be from one or more entities and include the person operating or using the system. This requirement should not pose unnecessary burden or delays and it could be sufficient that the separate verifications by the different persons are automatically recorded in the logs generated by the system.**

(49) High-risk AI systems should perform consistently throughout their lifecycle and meet an appropriate level of accuracy, robustness and cybersecurity in accordance with the generally acknowledged state of the art. The level of accuracy and accuracy metrics should be communicated to the users.

(50) The technical robustness is a key requirement for high-risk AI systems. They should be resilient **in relation to harmful or otherwise undesirable behaviour that may result from** ~~against risks connected to the~~ limitations **within the systems or the environment in which the systems operate** ~~of the system~~ (e.g. errors, faults, inconsistencies, unexpected situations)**. High-risk AI systems should therefore be designed and developed with appropriate technical solutions to prevent or minimize that harmful or otherwise undesirable behaviour, such as for instance mechanisms enabling the system to safely interrupt its operation (fail-safe plans) in the presence of certain anomalies or when operation takes place outside certain predetermined boundaries** ~~as well as against malicious actions that may compromise the security of the AI system and result in harmful or otherwise undesirable behaviour~~. Failure to protect against these risks could lead to safety impacts or negatively affect the fundamental rights, for example due to erroneous decisions or wrong or biased outputs generated by the AI system.

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

Obtenu pour vous par
Got for you by
agence europe

systems can leverage AI specific assets, such as training data sets (e.g. data poisoning) or trained models (e.g. adversarial attacks), or exploit vulnerabilities in the AI system's digital assets or the underlying ICT infrastructure. To ensure a level of cybersecurity appropriate to the risks, suitable measures should therefore be taken by the providers of high-risk AI systems, also taking into account as appropriate the underlying ICT infrastructure.

(52) As part of Union harmonisation legislation, rules applicable to the placing on the market, putting into service and use of high-risk AI systems should be laid down consistently with Regulation (EC) No 765/2008 of the European Parliament and of the Council[22] setting out the requirements for accreditation and the market surveillance of products, Decision No 768/2008/EC of the European Parliament and of the Council[23] on a common framework for the marketing of products and Regulation (EU) 2019/1020 of the European Parliament and of the Council[24] on market surveillance and compliance of products ('New Legislative Framework for the marketing of products').

(52a) In line with New Legislative Framework principles, specific obligations for relevant operators within the AI value chain should be set to ensure legal certainty and facilitate compliance with this Regulation. In certain situations those operators could act in more than one role at the same time and should therefore fufil cumulatively all relevant obligations associated with those roles. For example, an operator could act as a distributor and an importer at the same time.

(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.

(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. 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.

(54a) To ensure legal certainty, it is necessary to clarify that, under certain specific conditions, any natural or legal person should be considered a provider of a new high-risk AI system and therefore assume all the relevant obligations ~~under certain specific conditions~~. For example, this would be the case if that person puts its name or trademark on a high-risk AI system already placed on the market or put into service, or if that person modifies the intended purpose of an AI system which is not high-risk and is already placed on the market or put into service, in a way that makes the modified system a high-risk AI system. These provisions should apply without prejudice to more specific provisions established in certain New Legislative Framework sectorial legislation with which this Regulation should apply jointly. For example,

---

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

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

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

Obtenu pour vous par
Got for you by
agence europe

Article 16, paragraph 2 of Regulation 745/2017, establishing that certain changes should not be considered modifications of a device that could affect its compliance with the applicable requirements, should continue to apply to high-risk AI systems that are medical devices within the meaning of that Regulation.

(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 **product** 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.

(56a) For providers who are not established in the Union, the authorised representative plays a pivotal role in ensuring the compliance of the high-risk AI systems placed on the market or put into service in the Union by those providers and in serving as their contact person established in the Union. Given that pivotal role, and in order to ensure that responsibility is assumed for the purposes of enforcement of this Regulation, it is appropriate to make the authorised representative jointly and severally liable with the provider for defective high-risk AI systems. The liability of the authorised representative provided for in this Regulation is without prejudice to the provisions of Directive 85/374/EEC on liability for defective products.

(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 regard 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 users. Users 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. **These obligations <u>should be without prejudice to other user obligations in relation to high-risk AI systems under Union or national law, and</u> should not apply where the use is made in the course of a personal non-professional activity.**

(58a) ~~The obligations placed on various operators involved in the AI value chain under this Regulation should apply without prejudice to all other applicable Union and Member States laws aiming to protect fundamental rights and to regulate certain activities, products and services regardless of whether AI systems are used or not. In particular,~~ ~~i~~<u>I</u>t is appropriate to clarify that this Regulation does not affect the obligations of providers and users of AI systems in their role as data controllers or processors stemming from Union law on the protection of personal data in so far as the design, the development or the use of AI systems involves the processing of personal data. It is also appropriate to clarify that data subjects continue to enjoy all the rights and guarantees awarded to them by such Union law, including the rights related to solely automated

Obtenu pour vous par
Got for you by
agence europe

individual decision-making, including profiling. Harmonised rules for the placing on the market, the putting into service and the use of AI systems established under this Regulation should facilitate the effective implementation and enable the exercise of the data subjects' rights and other remedies guaranteed under Union law on the protection of personal data and of other fundamental rights.

(59) ~~It is appropriate to envisage that the user 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) ~~In the light of the complexity of the artificial intelligence value chain, relevant third parties, notably the ones involved in the sale and the supply of software, software tools and components, pre-trained models and data, or providers of network services, should cooperate, as appropriate, with providers and users to enable their compliance with the obligations under this Regulation and with competent authorities established under this Regulation.~~

(61) Standardisation should play a key role to provide technical solutions to providers to ensure compliance with this Regulation**, in line with the state of the art**. Compliance with harmonised standards as defined in Regulation (EU) No 1025/2012 of the European Parliament and of the Council[25]**, which are normally expected to reflect the state of the art,**should be a means for providers to demonstrate conformity with the requirements of this Regulation. However, ~~the Commission could adopt common technical specifications in areas where no harmonised standards exist or where they are insufficient.~~ **in the absence of relevant references to harmonised standards, the Commission should be able to establish, via implementing acts, common specifications as an exceptional fall back solution to facilitate the provider's obligation to comply with the requirements of this Regulation, when the standardisation process is blocked or when there are delays in the establishment of an appropriate harmonised standard. If such delay is due to the technical complexity of the standard in question, this should be considered by the Commission before contemplating the establishment of common specifications. An appropriate involvement of small and medium enterprises in the elaboration of standards supporting the implementation of this Regulation is essential to promote innovation and competitiveness in the field of artificial intelligence within the Union. Such involvement should be appropriately ensured in accordance with Article 5 and 6 of Regulation 1025/2012.**

(61a) It is appropriate that, without prejudice to the use of harmonised standards and common specifications, providers benefit from a presumption of conformity with the relevant requirement on data when their high-risk AI system has been trained and tested on data reflecting the specific geographical, behavioural or functional setting within which the AI system is intended to be used. Similarly, in line with Article 54(3) of Regulation (EU) 2019/881 of the European Parliament and of the Council, high-risk AI systems that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to that Regulation and the references of which have been published in the Official Journal of the European Union should be presumed to be in compliance with the cybersecurity requirement of this Regulation. This remains without prejudice to the voluntary nature of that cybersecurity scheme.

[25] 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).

Obtenu pour vous par
Got for you by
agence europe

(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.

(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. **With regard to high-risk AI systems related to products covered by Regulations 745/2017 and 746/2017 on medical devices, the applicability of the requirements of this Regulation should be without prejudice and take into account the risk management logic and benefit-risk assessment performed under the medical device framework.**

(64) Given the more extensive experience of professional pre-market certifiers in the field of product safety and the different nature of risks involved, it is appropriate 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~~ **remote** biometric identification of persons, for which the involvement of a notified body in the conformity assessment should be foreseen, to the extent they are not prohibited.

(65) In order to carry out third-party conformity assessment for AI systems intended to be used for the ~~remote~~ **remote** biometric identification of persons, notified bodies should be ~~designated~~ **notified** under this Regulation by the national competent authorities, provided they are compliant with a set of requirements, notably on independence, competence and absence of conflicts of interests. **Notification of those bodies should be sent by national competent authorities to the Commission and the other Member States by means of the electronic notification tool developed and managed by the Commission pursuant to Article R23 of Decision 768/2008.**

(66) In line with the commonly established notion of substantial modification for products regulated by Union harmonisation legislation, it is appropriate that **whenever a change occurs which may affect the compliance of a high risk AI system with this Regulation (e.g. change of operating system or software architecture~~, new or modified training datasets~~), or when the intended purpose of the system changes, that AI system should be considered a new AI system which should undergo** ~~an AI system undergoes~~ a new conformity assessment ~~whenever a change occurs which may affect the compliance of the system with this Regulation or when the intended purpose of the system changes~~. ~~In addition~~ **However**, **changes occuring to the algorithm and the performance of AI systems which continue to 'learn' after being placed on the market or put into service (i.e. automatically adapting how functions are carried out) should not constitute a**

Obtenu pour vous par
Got for you by
agence europe

substantial modification, provided that those changes have been pre-determined by the provider and assessed at the moment of the conformity assessment. ~~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 the 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.~~

(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. 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 and for society as a whole. It is thus appropriate that under exceptional reasons of public security or protection of life and health of natural persons and the protection of industrial and commercial property, Member States could authorise the placing on the market or putting into service of AI systems which have not undergone a conformity assessment.

(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 **themselves and information about** their high-risk AI system in a EU database, to be established and managed by the Commission. **Before using a high-risk AI system listed in Annex III, users of high-risk AI systems that are public authorities, agencies or bodies, with the exception of law enforcement, border control, immigration or asylum authorities, and authorities that are users of high-risk AI systems in the area of critical infrastructure shall also register themselves in such database and select the system that they envisage to use.** The Commission should be the controller of that database, in accordance with Regulation (EU) 2018/1725 of the European Parliament and of the Council[26]. 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.

(70) Certain AI systems intended to interact with natural persons or to generate content may pose specific risks of impersonation or deception irrespective of whether they qualify as high-risk or not. In certain circumstances, the use of these systems should therefore be subject to specific transparency obligations without prejudice to the requirements and obligations for high-risk AI systems. In particular, natural persons should be notified that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use. Moreover, natural persons should be notified when they are exposed **to systems that, by processing their biometric data, can identify or infer the emotions or intentions of those persons or assign them to specific categories. Such specific categories can relate to physical aspects, such as sex, age, hair colour, eye colour, tatoos, personal traits, ethnic origin or to personal preferences and interests such as sexual or political orientation.** ~~to an emotion recognition system or a biometric categorisation system~~. Such

[26] 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).

Obtenu pour vous par
Got for you by
agence europe

information and notifications should be provided in accessible formats for persons with disabilities. Further, users, who use an AI system to generate or manipulate image, audio or video content that appreciably resembles existing persons, places or events and would falsely appear to a person to be authentic, should disclose that the content has been artificially created or manipulated by labelling the artificial intelligence output accordingly and disclosing its artificial origin. **The compliance with the information obligations referred to above should not be interpreted as indicating that the use of the system or its output is lawful under this Regulation or other Union and Member State law and should be without prejudice to other transparency obligations for users of AI systems laid down in Union or national law. Furthermore it should also not be interpreted as indicating that the use of the system or its output impedes the right to freedom of expression and the right to freedom of the arts and sciences guaranteed in the Charter of Funadamental Rights of the EU, in particular where the content is part of an evidently creative, satirical, artistic or fictional work or programme, subject to appropriate safeguards for the rights and freedoms of third parties.**

~~**(70a) In the light of the nature and complexity of the value chain for AI systems, it is essential to clarify the role of persons who may contribute to the development of AI systems covered by this Regulation, without being providers and thus being obliged to comply with the obligations and requirements established herein. In particular, it is necessary to clarify that general purpose AI systems - understood as AI system that are able to perform generally applicable functions such as image/speech recognition, audio/video generation, pattern detection, question answering, translation etc. - should not be considered as having an intended purpose within the meaning of this Regulation. Therefore the placing on the market, putting into service or use of a general purpose AI system, irrespective of whether it is licensed as open source software or otherwise, should not, as such, trigger any of the requirements or obligations of this Regulation. However, if a person places on the market or puts into service under its own name or trademark or uses a general purpose AI system made available on the market for an intended purpose within the meaning of this Regulation, that person should be considered the provider of the AI system. Similarly, if a person integrates a general purpose AI system made available on the market, with or without modifying it, into an AI system that is subject to the provisions of this Regulation, that person should also be considered the provider of the latter AI system. The providers of general purpose AI systems and, as relevant, other third parties that may supply other software tools and components, including pre-trained models and data should cooperate, as appropriate, with providers and users to enable their compliance with the relevant obligations under this Regulation and with the competent authorities established under this Regulation.**~~

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

(72) The objectives of the **AI** regulatory sandboxes should be to foster AI innovation by establishing a controlled experimentation and testing environment in the development and pre-marketing phase with a view to ensuring compliance of the innovative AI systems with

Obtenu pour vous par
Got for you by
agence europe

this Regulation and other relevant Union and Member States legislation; to enhance legal certainty for innovators and the competent authorities' oversight and understanding of the opportunities, emerging risks and the impacts of AI use, and to accelerate access to markets, including by removing barriers for small and medium enterprises (SMEs)**, including** ~~and~~ start-ups. **The participation in the AI regulatory sandbox should focus on issues that raise legal uncertainty for providers and prospective providers to innovate,** ~~**and**~~ **experiment with AI in the Union and contribute to evidence-based regulatory learning. The supervision of the AI systems in the AI regulatory sandbox should therefore cover their development, training, testing and validation before the systems are placed on the market or put into service, as well as the notion and occurrence of substantial modification that may require a new conformity assessment procedure.** ~~**Access to the AI regulatory sandbox and regulatory supervision should be in principle free of charge without prejudice to exceptional costs that may be recovered by national authorities in a fair and proportionate manner, in particular in cases where the authorities have provided additional services for the actual development, testing and validation of the AI system such as technical or physical environment and tools for the testing, access to data, etc.**~~ **Where appropriate, national competent authorities establishing AI regulatory sandboxes should cooperate with other relevant authorities, including those supervising the protection of fundamental rights, and could allow for the involvement of other actors within the AI ecosystem such as national or European standardisation organisations, notified bodies, testing and experimentation facilities, research and experimentation labs, innovation hubs and relevant stakeholder and civil society organisations.** To ensure uniform implementation across the Union and economies of scale, it is appropriate to establish common rules for the regulatory sandboxes' implementation and a framework for cooperation between the relevant authorities involved in the supervision of the sandboxes. **AI regulatory sandboxes established under this Regulation should be without prejudice to other** ~~**existing**~~ **legislation allowing for the establishment of other sandboxes aiming at ensuring compliance with legislation other that this Regulation. Where appropriate, relevant competent authorities in charge of those other regulatory sandboxes should consider the benefits of using those sandboxes also for the purpose of ensuring compliance of AI systems with this Regulation. Upon agreement between the national competent authorities and the participants in the AI regulatory sandbox, testing in real world conditions may also be operated and supervised in the framework of the AI regulatory sandbox.**

(72-a) This Regulation should provide the legal basis **for the participants in the AI regulatory sandbox to** ~~for the~~ use ~~of~~ personal data collected ~~for other purposes~~ **for other purposes** for developing certain AI systems in the public interest within the AI regulatory sandbox, in line with Article 6**(4)(**~~**1)(c)**~~ **and 9(2)(g)** of Regulation (EU) 2016/679, and Article 5 **and 10** of Regulation (EU) 2018/1725, and without prejudice to Article**s 4(2) 8 and 10** of Directive (EU) 2016/680. ~~**This new legal basis under this Regulation is without prejudice to the possibility for participants to rely on other legal bases for processing of personal data under Articles 6(1) and 9(2) of Regulation (EU) 2016/679 and Articles 5 and 10(2) of Regulation (EU) 2018/1725.**~~ **All other obligations of data controllers and rights of data subjects under Regulation (EU) 2016/679, Regulation (EU) 2018/1725 and Directive (EU) 2016/680 remain applicable. In particular, this Regulation should not provide a legal basis in the meaning of Article 22(2)(b) of Regulation (EU) 2016/679 and Article 24(2)(b) of Regulation (EU) 2018/1725.** Participants 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 and fundamental rights that may arise during the development and experimentation in the

Obtenu pour vous par
Got for you by
agence europe

sandbox. The conduct of the participants in the sandbox should be taken into account when competent authorities decide whether to impose an administrative fine under Article 83(2) of Regulation 2016/679 and Article 57 of Directive 2016/680.
~~**AI regulatory sandboxes established under this Regulation should be without prejudice to existing legislation allowing for the establishment of other sandboxes aiming at ensuring compliance with legislation other that this Regulation. Upon agreement between the national competent authorities and the participants in the AI regulatory sandbox, testing in real world conditions may also be operated and supervised in the framework of the AI regulatory sandbox.**~~

(72a) In order to accelerate the process of development and placing on the market of high-risk AI systems listed in Annex III, it is important that providers or prospective providers of such systems may also benefit from a specific regime for testing those systems in real world conditions, without participating in an AI regulatory sandbox. However, in such cases and taking into account the possible consequences of such testing on individuals, it should be ensured that appropriate and sufficient guarantees and conditions are introduced by the Regulation for providers or prospective providers. Such guarantees should include, among others, requesting informed consent of natural persons to participate in testing in real world conditions, with the exception of law enforcement in cases where the seeking of informed consent would prevent the AI system from being tested. Consent of subjects to participate in such testing under this Regulation is distinct from and without prejudice to consent of data subjects for the processing of their personal data under the relevant data protection law.

(73) In order to promote and protect innovation, it is important that the interests of ~~small-scale~~**SME** providers and users of AI systems are taken into particular account. To this objective, Member States should develop initiatives, which are targeted at those operators, including on awareness raising and information communication. Moreover, the specific interests and needs of ~~small-scale~~**SME** providers shall be taken into account when ~~N~~**n**otified **b**~~B~~odies set conformity assessment fees. Translation costs related to mandatory documentation and communication with authorities may constitute a significant cost for providers and other operators, notably those of a smaller scale. Member States should possibly ensure that one of the languages determined and accepted by them for relevant providers' documentation and for communication with operators is one which is broadly understood by the largest possible number of cross-border users.

(73a) In order to promote and protect innovation, the AI-on demand platform, all relevant EU funding programmes and projects, such as Digital Europe Programme, Horizon Europe, implemented by the Commission and the Member States at national or EU level should contribute to the achievement of the objectives of this Regulation.

(74) **In particular, i**~~I~~n order to minimise the risks to implementation resulting from lack of knowledge and expertise in the market as well as to facilitate compliance of providers, **notably SMEs,** and notified bodies with their obligations under this Regulation, the AI-on demand platform, the European Digital Innovation Hubs and the Testing and Experimentation Facilities established by the Commission and the Member States at national or EU level should possibly contribute to the implementation of this Regulation. Within their respective mission and fields of competence, they may provide in particular technical and scientific support to providers and notified bodies.

(74a) Moreover, in order to ensure proportionality considering the very small size of some operators regarding costs of innovation, it is appropriate to exempt microenterprises from the most costly obligations, such as to establish a quality management system

Obtenu pour vous par
Got for you by
agence europe

which would reduce the administrative burden and the costs for those enterprises without affecting the level of protection and the need for compliance with the requirements for high-risk AI systems.

(75) It is appropriate that the Commission facilitates, to the extent possible, access to Testing and Experimentation Facilities to bodies, groups or laboratories established or accredited pursuant to any relevant Union harmonisation legislation and which fulfil tasks in the context of conformity assessment of products or devices covered by that Union harmonisation legislation. This is notably the case for expert panels, expert laboratories and reference laboratories in the field of medical devices pursuant to Regulation (EU) 2017/745 and Regulation (EU) 2017/746.

(76) In order to facilitate a smooth, effective and harmonised implementation of this Regulation a European Artificial Intelligence Board should be established. **The Board should reflect the various interests of the AI eco-system and be composed of representatives of the Member States** ~~**and of permanent experts representing different stakeholders**~~. **In order to ensure the involvement of relevant stakeholders, a standing subgroup of the Board should be created.** The Board should be responsible for a number of advisory tasks, including issuing opinions, recommendations, advice or **contributing to** guidance on matters related to the implementation of this Regulation, including on **enforcement matters,** technical specifications or existing standards regarding the requirements established in this Regulation and providing advice to ~~**and assisting**~~ the Commission **and the Member States and their national competent authorities** on specific questions related to artificial intelligence. **In order to give some flexibility to Member States in the designation of their representatives in the AI Board, such representatives may be any persons belonging to** ~~**or**~~ **public entities who should have the relevant competences and powers to facilitate coordination at national level and contribute to the achievement of the Board's tasks. The Board should establish two standing sub-groups to provide a platform for cooperation and exchange among market surveillance authorities and notifying authorities on issues related respectively to market surveillance and notified bodies. The standing subgroup for market surveillance should act as the Administrative Cooperation Group (ADCO) for this Regulation in the meaning of Article 30 of Regulation (EU) 2019/1020. In line with the role and tasks of the Commission pursuant to Article 33 of Regulation (EU) 2019/1020, the Commission** ~~**may**~~ **should support the activities of the standing subgroup for market surveillance by undertaking market evaluations or studies, notably with a view to identifying aspects of this Regulation requiring specific and urgent coordination among market surveillance authorities. The Board may establish other standing or temporary sub-groups as appropriate for the purpose of examining specific issues. The Board should also cooperate, as appropriate, with relevant EU bodies, experts groups and networks active in the context of relevant EU legislation, including in particular those active under relevant EU regulation on digital products and services.**

(76a) The Commission should actively support the Member States and operators in the implementation and enforcement of this Regulation. In this regard it should develop guidelines on particular topics aiming at facilitating the application of this Regulation, while paying particular attention to the needs of SMEs and start-us in sectors most likely to be affected. In order to support adequate enforcement and the capacities of the Member States, Union testing facilities on AI and a pool of relevant experts should be established and made available to the Member States.

(77) Member States hold a key role in the application and enforcement of this Regulation. In this respect, each Member State should designate one or more national competent authorities for

Obtenu pour vous par
Got for you by
agence europe

the purpose of supervising the application and implementation of this Regulation. ~~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, in each Member State one national authority should be designated as national supervisory authority.~~ **Member States may decide to appoint any kind of public entity to perform the tasks of the national competent authorities within the meaning of this Regulation, in accordance with their specific national organisational characteristics and needs.**

(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' 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 protecting fundamental rights~~ resulting from the use of their AI systems.

(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. **Market surveillance authorities designated pursuant to this Regulation should have all enforcement powers under this Regulation and Regulation (EU) 2019/1020 <u>and should exercise their powers and carry out their duties independently, impartially and without bias</u>. Although the majority of AI systems are not subject to specific requirements and obligations under this Regualtion, market surveillance authorities may take measures in relation to all AI systems when they present a risk in accordance with this Regulation. <u>Due to the specific nature of</u> ~~For~~ Union institutions, agencies and bodies falling within the scope of this Regulation, it is appropriate to designate the European Data Protection Supervisor as a competent market surveillance authority <u>for them</u>. <u>This should be without prejudice to the designation of national competent authorities by the Member States.</u> Market surveillance activities should not affect the ability of the supervised entities to carry out their tasks independently, when such independence is required by Union law.**

(79a) 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. A specific safeguard procedure should be set for ensuring adequate and timely enforcement against AI systems presenting a risk to health, safety and fundamental rights. The procedure for such AI systems presenting a risk should be applied to high-risk AI systems presenting a risk, prohibited systems which have been placed on the market, put into service or used in violation of the prohibited practices laid down in this Regulation and AI systems which have been made available in violation of the transparency requirements laid down in this Regulation and present a risk.

(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 authorities responsible for the supervision and enforcement of the financial services legislation~~,~~

Obtenu pour vous par
Got for you by
agence europe

~~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 **unless Member States decide to designate another authority to fulfill these market surveillance tasks. Those competent authorities should have all powers under this Regulation and Regulation (EU) 2019/1020 on market surveillance to enforce the requirements and obligations of this Regulation, including powers to carry our ex post market surveillance activities that can be integrated, as appropriate, into their existing supervisory mechanisms and procedures under the relevant Union financial services legislation. It is appropriate to envisage that, when acting as market surveillance authorities under this Regulation, the national authorities responsible for the supervision of credit institutions regulated under Directive 2013/36/EU, which are participating in the Single Supervisory Mechanism (SSM) established by Council Regulation No ~~1204~~ 1024/2013, should report, without delay, to the European Central Bank any information identified in the course of their market surveillance activities that may be of potential interest for the European Central Bank's prudential supervisory tasks as specified in that Regulation. ~~in Council Regulation (EU) No 1204/2013 establishing the Single Supervisory Mechanism (SSM).~~** 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[27], it is also appropriate to integrate ~~the conformity assessment procedure an~~d 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 users of high-risk AI systems to the extent that these apply to credit institutions regulated by Directive 2013/36/EU. **The same regime should apply to insurance and re-insurance undertakings and insurance holding companies under Directive 2009/138/EU (Solvency II) and the insurance intermediaries under Directive 2016/97/EU and other types of financial institutions subject to requirements regarding internal governance, arrangements or processes established pursuant to the relevant Union financial services legislation to ensure consistency and equal treatment in the financial sector.**

(81) The development of AI systems other than high-risk AI systems in accordance with the requirements of this Regulation may lead to a larger uptake of trustworthy artificial intelligence in the Union. Providers of non-high-risk AI systems should be encouraged to create codes of conduct intended to foster the voluntary application of the ~~mandatory~~ requirements applicable to high-risk AI systems**, adapted in light of the intended purpose of the systems and the lower risk involved**. Providers should also be encouraged to apply on a voluntary basis additional requirements related, for example, to environmental sustainability, accessibility to persons with disability, stakeholders' participation in the design and development of AI systems, and diversity of the development teams. The Commission may develop initiatives, including of a sectorial nature, to facilitate the lowering of technical barriers hindering cross-border exchange of data for AI development, including on data access infrastructure, semantic and technical interoperability of different types of data.

---

[27] 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).

Obtenu pour vous par
Got for you by
agence europe

(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 herein 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[28] would apply as a safety net.

(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 respect the confidentiality of information and data obtained in carrying out their tasks**, in accordance with Union or national law**.

(84) Member States should take all necessary measures to ensure that the provisions of this Regulation are implemented, including by laying down effective, proportionate and dissuasive penalties for their infringement, **and in respect of the *ne bis in idem* principle**. For certain specific infringements, Member States should take into account the margins and criteria set out in this Regulation. 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.

(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[29]. 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. **Such consultations and advisory support should also be carried out in the framework of the activities of the AI Board and its subgroups.**

(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[30]. **It is of particular importance that, in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making, whenever broader expertise is needed in the early preparation of draft implementing acts, the Commission makes use of expert groups, consults targeted stakeholders or carries out public consultations, as appropriate. Such consultations and advisory support should also be carried out in the framework of the activities of the AI Board**

---

[28] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (OJ L 11, 15.1.2002, p. 4).

[29] OJ L 123, 12.5.2016, p. 1.

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

Obtenu pour vous par
Got for you by
agence europe

and its subgroups, including the preparation of implementing acts in relation to Articles 4, 4b and 6.

(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) In order to ensure legal certainty, ensure an appropriate adaptation period for operators and avoid disruption to the market, including by ensuring continuity of the use of AI systems, it is appropriate that this Regulation applies to the high-risk AI systems that have been placed on the market or put into service before the general date of application thereof, only if, from that date, those systems are subject to significant changes in their design or intended purpose. It is appropriate to clarify that, in this respect, the concept of significant change should be understood as equivalent in substance to the notion of substantial modification, which is used with regard only to high-risk AI systems as defined in this Regulation.

(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 […]".

HAVE ADOPTED THIS REGULATION:

TITLE I

GENERAL PROVISIONS

Article 1
Subject matter

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;

(a) prohibitions of certain artificial intelligence practices;

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

(c) 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~~;

Obtenu pour vous par
Got for you by
agence europe

(d) rules on market monitoring**,** ~~and~~ **market** surveillance **and governance**~~.;~~

(e) measures in support of innovation.

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 **physically present or** established within the Union or in a third country;

(b) users of AI systems **who are physically present or established** ~~located~~ within the Union;

(c) providers and users of AI systems ~~that~~ **who are physically present or established** ~~located~~ in a third country, where the output produced by the system is used in the Union;

(d) **importers and distributors of AI systems;**

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

(f) authorised representatives of providers, which are established in the Union;

2. For **AI systems classified as** high-risk AI **systems in accordance with Articles 6(1) and 6(2) related to products covered by Union harmonisation legislation listed in Annex II, section B** ~~systems that are safety components of products or systems, or which are themselves products or systems, falling within the scope of the following acts~~ only Article~~s~~ ~~**53 and**~~ 84 of this Regulation shall apply~~.:~~**. Article 53 shall apply only insofar as the requirements for high-risk AI systems under this Regulation have been integrated under that Union harmonisation legislation.**

~~(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 **if and insofar** ~~developed~~ **placed on the market, ~~or~~ put into service, or used with or without modification of such systems** ~~or used~~ ~~[exclusively]~~ for **the purpose of activities which fall outside the scope of Union law, and in any event activities concerning** military**, defence or national security** ~~purposes~~**, regardless of the type of entity carrying out those activities**.

In addition, this Regulation shall not apply to AI systems which are not placed on the market or put into service in the Union, where the output is used in the Union for the

Obtenu pour vous par
Got for you by
agence europe

purpose of activities which fall outside the scope of Union law, and in any event activities concerning military, defence or national security, regardless of the type of entity carrying out those activities.

~~**3a. Entities carrying out activities referred to in paragraph 3, shall not be subject to user's obligations provided for in this Regulation.**~~

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 agreements for law enforcement and judicial cooperation with the Union or with one or more Member States.

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~~**4** of Directive 2000/31/EC of the European Parliament and of the Council[31] [*as to be replaced by the corresponding provisions of the Digital Services Act*].

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

7. **This Regulation shall not apply to ~~affect~~ any research and development activity regarding AI systems. ~~in so far as such activity does not lead to or entail placing an AI system on the market or putting it into service~~.**

8. This Regulation shall not apply to obligations of users who are natural persons using AI systems in the course of a purely personal non-professional activity, except Article 52.

Article 3
Definitions

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

(1) ~~'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;~~

~~**'artificial intelligence system' (AI system) means a system that**~~

~~**(i) receives machine and/or human-based data and inputs,**~~

~~**(ii) infers how to achieve a given set of human-defined objectives using learning, reasoning or modelling implemented with the techniques and approaches listed in Annex I, and**~~

~~**(iii) generates outputs in the form of content (generative AI systems), predictions, recommendations or decisions, which influence the environments it interacts with;**~~

'artificial intelligence system' (AI system) means a system that is designed to operate with ~~a certain level~~ elements of autonomy and that, based on machine and/or

[31] 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).

Obtenu pour vous par
Got for you by
agence europe

human-provided data and inputs, infers how to achieve a given set of ~~human-defined~~ objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts;

(1a) 'life cycle of an AI system' means the duration of an AI system, from design through retirement. Without prejudice to the powers of the market surveillance authorities, ~~S~~such retirement may happen at any point in time during the post-market monitoring phase upon the decision of the provider and implies that the system may not be used further. An AI system lifecycle is also ended by a substantial modification to the AI system made by the provider or any other natural or legal person, in which case the substantially modified AI system shall be considered as a new AI system.

(1b) 'general purpose AI system' means an AI system that - irrespective of how ~~the modality in which~~ it is placed on the market or put into service, including as open source software - is intended by the provider to perform generally applicable functions such as image and speech recognition, audio and video generation, pattern detection, question answering, translation and others; a general purpose AI system may be used in a plurality of contexts and be integrated in a plurality of other AI systems;

(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 **and places that system on the market or puts it into service** ~~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/EC[32];~~

(3a) 'small and medium-sized enterprise' (SMEs) means an enterprise as defined in the Annex of Commission Recommendation 2003/361/EC concerning the definition of micro, small and medium-sized enterprises;

(4) 'user' means any natural or legal person, **including a** public authority, agency or other body**,** ~~using an AI system under its~~ **under whose** authority **the system is used;**~~, 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~~ **physically present or established** in the Union who has received **and accepted** 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;

(5a) 'product manufacturer' means a manufacturer within the meaning of any of the Union harmonisation legislation listed in Annex II;

(6) 'importer' means any natural or legal person ~~established~~ **physically present or 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~~;

---

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

Obtenu pour vous par
Got for you by
agence europe

(8) 'operator' means the provider**, the product manufacturer,** the user, the authorised representative, the importer ~~and~~ **or** the distributor;

(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 user or for own use ~~on the Union market~~ **in the Union** for its intended purpose~~;~~**. ~~By way of derogation, field testing taking place under the conditions of Article 64a shall not be considered as putting into service;~~**

(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**; ~~general purpose AI systems shall not be considered as having an intended purpose within the meaning of this Regulation;~~**

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

(14) 'safety component of a product or system' means a component of a product or of a system which fulfils a safety function for that product or system 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 user of in particular an AI system's intended purpose and proper use ~~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 **or taking it out of service or disabling the use** of an AI system made available to users;

(17) 'withdrawal of an AI system' means any measure aimed at preventing **an AI system in the supply chain being made available on the market**~~. 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) **'conformity assessment' means the process of verifying whether the requirements set out in Title III, Chapter 2 of this Regulation relating to a~~n~~ high-risk AI system have been fulfilled;** ~~'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 verifying whether the requirements set out in Title III, Chapter 2 of this Regulation relating to an AI system have been fulfilled;~~ **'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;**

Obtenu pour vous par
Got for you by
agence europe

(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 designated in accordance with this Regulation and other relevant Union harmonisation legislation;

(23) ‘substantial modification’ means a change to the AI system following its placing on the market or putting into service which affects the compliance of the AI system with the requirements set out in Title III, Chapter 2 of this Regulation, or ~~results in~~ a modification to the intended purpose for which the AI system has been assessed~~;~~**. 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.**

(24) ‘CE marking of conformity’ (CE marking) means a marking by which a provider indicates that an AI system is in conformity with the requirements set out in Title III, Chapter 2 **or in Article 4b** of this Regulation and other applicable Union ~~legislation~~ **legal act** harmonising the conditions for the marketing of products (‘Union harmonisation legislation’) providing for its affixing;

(25) ‘post-market monitoring **system**’ 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 **set of technical specifications** ~~document~~, **as defined in point 4 of Article 2 of Regulation (EU) No 1025/2012**, other than a standard, ~~containing solutions,~~ providing ~~a~~ **~~mandatory~~** 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 overfitting; whereas the validation dataset can be 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 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;

Obtenu pour vous par
Got for you by
agence europe

(34) ‘emotion recognition system’ means an AI system for the purpose of identifying or inferring **psychological states,** emotions or intentions of natural persons on the basis of their biometric data;

(35) ‘biometric categorisation system’ means an AI system for the purpose of assigning natural persons to specific categories~~, such as sex, age, hair colour, eye colour, tattoos,~~ ~~**health, personal traits,** ethnic origin or sexual or political orientation~~, on the basis of their biometric data;

(36) ‘~~remote~~ **remote** biometric identification system’ means an AI system for the purpose of identifying **natural persons**~~, at a distance~~ **typically at a distance, without their active involvement,** through the comparison of a person’s biometric data with the biometric data contained in a reference ~~database~~ **data repository**~~**, excluding verification/authentification systems whose sole purpose is to confirm that a specific natural person is the person he or she claims to be or is deemed to be, and or systems that are used to confirm the identity of a natural person for the sole purpose of having access to a service, a device or premises**~~; and without prior knowledge of the user of the AI system whether the person will be present and can be identified ;~~

(37) ‘‘real-time’ ~~remote~~ **remote** biometric identification system’ means a ~~remote~~ **remote** biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur **instantaneously or near instantaneously** ~~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 **an undetermined number of natural persons** ~~the public~~, regardless of whether certain conditions **or circumstances** for access **have been predetermined, and regardless of the potential capacity restrictions** ~~**may apply**~~;

(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 the authority to which a Member State assigns the responsibility for the implementation and application of this Regulation, for coordinating~~ ~~**the related** activities **of the national competent authorities** entrusted to that Member State, for acting as the single contact point for the Commission, and for representing the Member State at the European Artificial Intelligence Board;~~

(43) ‘national competent authority’ **means any of the following:** ~~the national supervisory authority,~~ the notifying authority~~**, and**~~ **and** the market surveillance authority~~;~~**. As regards**

Obtenu pour vous par
Got for you by
agence europe

AI systems put into service or used by EU institutions, agencies, offices and bodies, the European Data Protection Supervisor~~PDS~~ shall fulfil the responsibilities that in the Member States are entrusted to the national competent authority and, as relevant, any reference to national competent authorities or market surveillance authorities in this Regulation shall be understood as referring to the European Data Protection Supervisor ~~act as a national competent authority, for the purposes 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.

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

(d) serious damage to property or the environment;

(45) 'critical infrastructure' means an asset, system or part thereof which is necessary for the delivery of a service that is essential for the maintenance of vital societal functions or economic activities within the meaning of Article 2(4) and (5) of Directive ...../..... on the resilience of critical entities;

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

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

(48) '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 with a view to gathering reliable and robust data and to assessing and verifying the conformity of the AI system with the requirements of this Regulation; testing in real world conditions shall not be considered as placing the AI system on the market or putting it into service within the meaning of this Regulation, provided that all conditions under Article 53 or Article 54a are fulfilled;

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

(50) 'subject' for the purpose of real world testing means a natural person who participates in ~~a real world~~ testing in real world conditions;

(51) 'informed consent' means a subject's free and voluntary expression of his or her willingness to participate in a particular testing in real world conditions, after having been informed of all aspects of the testing that are relevant to the subject's decision to participate; in the case of minors and of incapacitated subjects, the informed consent shall be given by their legally designated representative;

(52) 'AI regulatory sandbox' means a concrete framework set up by a national competent authority which offers providers or prospective providers of AI systems the possibility to develop, train, validate and test, where appropriate in real world conditions, an innovative AI system, pursuant to a specific plan for a limited time under regulatory supervision.

Obtenu pour vous par
Got for you by
agence europe

Article 4

~~Amendments to Annex I~~Implementing acts

~~The Commission is empowered to adopt delegated acts~~ **In order to ensure uniform conditions for the implementation of this Regulation as regards machine learning approaches and logic- and knowledged based approaches referred to in Article 3(1), the Commission may adopt implementing acts to specify the technical elements of those approaches, taking into account market and technological developments. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74(2).** ~~in accordance with Article 73 to amend the list of techniques and approaches listed in Annex I **within the scope of the definition of an AI system as provided for in Article 3(1)**, 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.~~

TITLE IA

GENERAL PURPOSE AI SYSTEMS

Article 4a

Compliance of general purpose AI systems with this Regulation

1. **Without prejudice to Articles 5,~~and~~ 52, 53 and 69 of this Regulation, general purpose AI systems shall only comply with the requirements and obligations set out in Article 4b.**

2. **Such requirements and obligations shall apply irrespective of whether the general purpose AI system is placed on the market or put into service as a pre-trained model and whether further fine-tuning of the model is to be performed by the user of the general purpose AI system.**

Article 4b

Requirements for general purpose AI systems and obligations for providers of such systems

1. **General purpose AI systems which may be used as high risk AI systems or as components of ~~AI~~ high risk AI systems in the meaning of Article 6, shall comply with the requirements established in Title III, Chapter 2 of this Regulation as from the date of application of the implementing acts adopted by the Commission in accordance with the examination procedure referred to in Article 74(2) no later than 18 months after the entry into force of this Regulation. Those implementing acts shall specify and adapt the application of the requirements established in Title III, Chapter 2 to general purpose AI systems in the light of their characteristics, technical feasibility, specificities of the AI value chain and of market and technological developments. ~~Articles, 9, 10, 11, 13(2) and 13(3)(a) to (c) and 13(3)(e) and 15 of this Regulation~~. 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~~.**

Obtenu pour vous par
Got for you by
agence europe

2. Providers of general purpose AI systems referred to in paragraph 1 shall comply with the obligations set out in Articles 16aa, 16e, 16f, 16g, 16i, 16j, 25, 48 and 61.

3. For the purpose of complying with the obligations set out in Article 16e, providers shall follow the conformity assessment procedure based on internal control set out in Annex VI, points 3 and 4.

4. Providers of such systems shall also keep the technical documentation referred to in Article 11 at the disposal of the national competent authorities for a period ending ten years after the general purpose AI system is placed on the Union market or put into service in the Union.

5. Providers of general purpose AI systems shall cooperate with and provide the necessary information to other providers intending to put into service or place such systems on the Union market as high-risk AI systems or as components of high-risk AI systems, with a view to enabling the latter to comply with their obligations under this Regulation. Such cooperation between providers shall preserve, as appropriate, intellectual property rights, and confidential business information or trade secrets in accordance with Article 70. In order to ensure uniform conditions for the implementation of this Regulation as regards the information to be shared by the providers of general purpose AI systems, the Commission may adopt implementing acts in accordance with the examination procedure referred to in Article 74(2).

6. **In complying with the requirements and obligations referred to in paragraphs 1, 2 and 3:**

- any reference to the intended purpose shall be understood as referring to possible use of the general purpose AI systems as high risk AI systems or as components of AI high risk systems in the meaning of Article 6;

- any reference to the requirements for high-risk AI systems in Chapter II, Title III shall be understood as referring only to the requirements set out in the present Article.

Article 4c
Exceptions to Article 4b

1. Article 4b shall not apply when the provider has explicitly excluded ~~any~~ all high-risk uses in the instructions of use or information accompanying the general purpose AI system.

2. Such exclusion shall be made in good faith and shall not be deemed justified if the provider has sufficient reasons to consider that the system may be misused.

3. When the provider detects or is informed about ~~statistically significant trends of~~ market misuse they shall take all necessary and proportionate measures to prevent such further misuse, in particular taking into account the scale of the misuse and the seriousness of the associated risks.

Obtenu pour vous par
Got for you by
agence europe

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 **with the objective to or the effect of** ~~in order to~~ materially distort**ing** a person's behaviour in a manner that causes or is **reasonably** likely to cause that person or another person physical or psychological harm;

(b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, ~~physical or mental~~ disability **or a specific social or economic situation**, **with the objective to or the effect of** ~~in order to~~ materially distort**ing** the behaviour of a person pertaining to that group in a manner that causes or is **reasonably** likely to cause that person or another person physical or psychological harm;

(c) the placing on the market, putting into service or use of AI systems ~~by public authorities or on their behalf~~ for the evaluation or classification ~~of the trustworthiness~~ of natural persons over a certain period of time based on their social behaviour or known 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 ~~whole~~ groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;

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

(d) the use of 'real-time' ~~remote~~ **remote** biometric identification systems in publicly accessible spaces **by law enforcement authorities or on their behalf** 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 **and** substantial ~~and imminent~~ threat to **the critical infrastructure,** life**, health** or physical safety of natural persons or **the prevention** of ~~a~~ terrorist attack**s**;

(iii) the ~~detection,~~ localisation~~,~~ **or** identification ~~or prosecution~~ of a **natural person for the purposes of conducting a criminal investigation, prosecution or executing a criminal penalty for offences** ~~perpetrator~~**,** ~~or~~ ~~suspect or convict of a criminal offence~~ referred to in Article 2(2) of Council Framework

Obtenu pour vous par
Got for you by
agence europe

Decision 2002/584/JHA[33] and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, **or other specific offences punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least five years,** as determined by the law of that Member State.

2. The use of 'real-time' ~~remote~~ **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~~ **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~~ **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~~ **provided that, such authorisation shall be requested without undue delay during ~~its~~ use of the AI system, and if such authorisation is rejected, its use shall be stopped with immediate effect.**

   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~~ **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~~ **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 **and reporting** relating to, the authorisations referred to in paragraph 3. Those rules shall also specify in respect of which of the objectives listed in paragraph 1, 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.

4a. ~~**The prohibition mentioned in Article 5(1)(d) shall not apply to situations where the person refuses or is not a capacity to disclose his or her identity in front of the law**~~

[33] 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).

Obtenu pour vous par
Got for you by
agence europe

~~**enforcement authority in publicly accessible spaces when that authority is authorised by Union or national law to carry out such identity checks.**~~ ~~**The prohibition mentioned in Article 5(1)(d) is without prejudice to the use of information systems by law enforcement, migration or asylum authorities of systems referred to in annex IX where these authorities are authorized by Union or national law to carry out identity checks.**~~

Obtenu pour vous par
Got for you by
agence europe

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 is itself a product, covered by the Union harmonisation legislation listed in Annex II;~~

~~(b) the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or 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 referred to in Annex III shall also be considered high-risk.~~

1. **An AI system that is itself a product covered by the Union harmonisation legislation listed in Annex II shall be considered as high risk if it is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the above mentioned legislation.**

2. **An AI system intended to be used as a safety component of a product covered by the legislation referred to in paragraph 1 shall be considered as high risk if it is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to above mentioned legislation. This provision shall apply irrespective of whether the AI system is placed on the market or put into service independently from the product.**

3. **AI systems referred to in Annex III shall be considered high-risk ~~if~~ unless ~~in any of the following cases:~~**

~~(a) the output of the system is immediately effective with respect to the intended purpose of the system without the need for a human to validate it;~~

~~(b)~~ the output of the system ~~consists of information that constitutes the sole basis or~~ is ~~not~~ purely accessory in respect of the relevant action or decision to be taken ~~by the human,~~ and may therefore lead to a significant risk to the health, safety or fundamental rights.

In order to ensure uniform conditions for the implementation of this Regulation, the Commission shall, no later than one year after the entry into force of this Regulation, adopt implementing acts to specify ~~further~~ the circumstances where the output of AI systems referred to in Annex III would be purely accessory in respect of the relevant

Obtenu pour vous par
Got for you by
agence europe

action or decision to be taken ~~**nature of the information across the relevant high-risk AI systems referred to in Annex III**~~**. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74, paragraph 2.**

Article 7
Amendments to Annex III

1. The Commission is empowered to adopt delegated acts in accordance with Article 73 to ~~update~~ **amend** the list in Annex III by adding high-risk AI systems where both of the following conditions are fulfilled:

   (a) the AI systems are intended to be used in any of the areas listed in points 1 to 8 of Annex III;

   (b) the AI systems pose a risk of harm to the health and safety, or a risk of adverse impact on fundamental rights, that 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.

2. When assessing for the purposes of paragraph 1 whether an AI system poses a risk of harm to the health and safety or a risk of adverse impact on fundamental rights that is equivalent to or greater than the risk of harm posed by the high-risk AI systems already referred to in Annex III, the Commission shall take into account the following criteria:

   (a) the intended purpose of the AI system;

   (b) the extent to which an AI system has been used or is likely to be used;

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

   (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;

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

   (f) the extent to which potentially harmed or adversely impacted persons are in a vulnerable position in relation to the user of an AI system, in particular due to an imbalance of power, knowledge, economic or social circumstances, or age;

   (g) the extent to which the outcome produced with an AI system is **not** easily reversible, whereby outcomes having an impact on the health or safety of persons shall not be considered as easily reversible;

   (h) the extent to which existing Union legislation provides for:

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

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

   (i) the magnitude and likelihood of benefit of the AI use for individuals, groups, or society at large.

Obtenu pour vous par
Got for you by
agence europe

3. The Commission is empowered to adopt delegated acts in accordance with Article 73 to amend the list in Annex III by ~~deleting~~ removing high-risk AI systems where both of the following conditions are fulfilled:

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

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

CHAPTER 2

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**, taking into account the generally acknowledged state of the art~~, including as reflected in relevant harmonised standards or common specifications~~**.

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

Article 9
Risk management system

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

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

(a) identification and analysis of the known and foreseeable risks **most likely to occur to health, safety and fundamental rights in view of the intended purpose of the high-risk AI system** ~~associated with each high-risk AI system~~;

~~(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 other possibly arising risks based on the analysis of data gathered from the post-market monitoring system referred to in Article 61;

(d) adoption of suitable risk management measures in accordance with the provisions of the following paragraphs.

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

Obtenu pour vous par
Got for you by
agence europe

3. The risk management measures referred to in paragraph 2, point (d) shall give due consideration to the effects and possible interaction resulting from the combined application of the requirements set out in this Chapter 2**, with a view to minimising risks more effectively while achieving an appropriate balance in implementing the measures to fulfil those 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 (d) shall be such that any residual risk associated with each hazard as well as the overall residual risk of the high-risk AI systems is judged 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 shall be communicated to the user.~~

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

   (a) elimination or reduction of ~~**identified and evaluated**~~ risks **identified and evaluated pursuant to paragraph 2** as far as possible through adequate design and development **of the high risk AI system**;

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

   (c) provision of adequate 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 users.

   With a view to ~~In~~ eliminating or reducing risks related to the use of the high-risk AI system, due consideration shall be given to the technical knowledge, experience, education, training to be expected by the user and the environment in which the system is intended to be used.

5. High-risk AI systems shall be tested **in order to** ~~for the purposes of identifying the most appropriate risk management measures. Testing shall~~ ensure that high-risk AI systems perform ~~consistently for~~ **in a manner that is consistent with** 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~~. **Testing procedures may include testing in real world conditions in accordance with Article 54a.**

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 preliminarily defined metrics and probabilistic thresholds that are appropriate to the intended purpose of the high-risk AI system.

8. ~~When implementing t~~**T**he risk management system described in paragraphs 1 to 7 **shall give** specific consideration **to** ~~shall be given to~~ whether the high-risk AI system is likely to be accessed by or have an impact on **persons under the age of 18** ~~children~~.

9. For **providers of high-risk AI systems that are** ~~credit institutions~~ **subject to requirements regarding internal risk management processes under relevant sectorial Union law** ~~regulated by Directive 2013/36/EU~~, the aspects described in paragraphs 1 to 8 **may** ~~shall~~ be part of the risk management procedures established ~~by those institutions~~ pursuant to **that law** ~~Article 74 of that Directive~~.

Obtenu pour vous par
Got for you by
agence europe

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.

2. Training, validation and testing data sets shall be subject to appropriate data governance and management practices. Those practices shall concern in particular,

   (a) the relevant design choices;

   (b) data collection **processes**;

   (c) relevant data preparation processing operations, such as annotation, labelling, cleaning, 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 prior 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 health and safety of natural persons or lead to discrimination prohibited by Union law**;

   (g) the identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed.

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

4. Training, validation and testing data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, 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 bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may 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 measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.

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

   ~~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. In order to comply with the requirements laid out in this Article, the data minimisation principle referred to in Article 5 paragraph 1c of Regulation (EU) 2016/679 shall be applied with consideration for the full life cycle of the system.**~~

Obtenu pour vous par
Got for you by
agence europe

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 competent authorities and notified bodies with all the necessary information **in a clear and comprehensive form** to assess the compliance of the AI system with those requirements. It shall contain, at a minimum, the elements set out in Annex IV **or, in the case of SMEs, including ~~and~~ start-ups, any equivalent documentation meeting the same objectives, unless deemed inappropriate by ~~subject to approval of~~ the competent 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 Annex IV 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.

Article 12
Record-keeping

1. High-risk AI systems shall ~~be designed and developed with capabilities enabling~~ **technically allow for** the automatic recording of events ('logs') **over the duration of the life cycle of the system** ~~while the high-risk AI systems is operating~~. ~~Those logging capabilities shall conform to recognised standards or common specifications.~~

2. ~~The logging capabilities shall ensure~~ **In order to ensure** a level of traceability of the AI system's functioning ~~throughout its lifecycle~~ that is appropriate to the intended purpose of the system**,**~~. 3. In particular,~~ logging capabilities shall enable the **recording of events relevant for** ~~monitoring of the operation of the high-risk AI system with respect to the occurrence of~~

   (i) identification of situations that may result in the AI system presenting a risk within the meaning of Article 65(1) or ~~lead to~~ **in** a substantial modification**;**~~, and~~

   (ii) ~~facilitate~~ **facilitation of** the post-market monitoring referred to in Article 61~~.~~**; and**

   (iii) monitoring of the operation of high-risk AI systems referred to in Article 29(4).

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;

Obtenu pour vous par
Got for you by
agence europe

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

Article 13
Transparency and provision of information to users

1. High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent ~~to enable users to interpret the system's output and use it appropriately. An appropriate type and degree of transparency shall be ensured,~~ with a view to achieving compliance with the relevant obligations of the user and of the provider set out in Chapter 3 of this Title **and enabling users to understand and use the system appropriately**.

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

3. The information referred to in paragraph 2 shall specify:

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

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

(i) its intended purpose**, inclusive of the specific geographical, behavioural or functional setting within which the high-risk AI system is intended to be used**;

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

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

(iv) **when appropriate,** its ~~performance~~ **behaviour regarding specific** ~~as regards the~~ persons or groups of persons on which the system is intended to be used;

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

(vi) when appropriate, description of the expected output of the system.

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

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

Obtenu pour vous par
Got for you by
agence europe

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

(f) a description of the mechanism included within the AI system that allows users to properly collect, store and interpret the logs, where relevant.

Article 14
Human oversight

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

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

3. Human oversight shall be ensured through either one or all of the following **types of** measures:

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

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

4. ~~The measures referred to in paragraph 3 shall enable the individuals~~ **For the purpose of implementing paragraphs 1 to 3, the high-risk AI system shall be provided to the user in such a way that natural persons** to whom human oversight is assigned **are enabled,** ~~to do the following~~, as appropriate **and proportionate** to the circumstances:

(a) ~~fully~~ **to** understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation~~, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible~~;

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

(c) ~~be able~~ to correctly interpret the high-risk AI system's output, taking into account **for example** ~~in particular~~ ~~the characteristics of the system and~~ the interpretation tools and methods available;

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

(e) ~~be able~~ to intervene on the operation of the high-risk AI system or interrupt the system through a "stop" button or a similar procedure.

5. For high-risk AI systems referred to in point 1(a) of Annex III, the measures referred to in paragraph 3 shall be such as to ensure that, in addition, no action or decision is taken by

Obtenu pour vous par
Got for you by
agence europe

the user on the basis of the identification resulting from the system unless this has been **separately** verified and confirmed by at least two natural persons. **The requirement for a separate verification <u>by at least two natural persons</u> shall not apply to high risk AI systems <u>used for the purpose of law enforcement, migration,</u> border control <u>or asylum</u>, in cases where Union or national law considers the application of this requirement to be disproportionate.**

Article 15
Accuracy, robustness and cybersecurity

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

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

3. High-risk AI systems shall be resilient as regards errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems.

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

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

4. High-risk AI systems shall be resilient as regards attempts by unauthorised third parties to alter their use or performance by exploiting the system vulnerabilities.

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

   The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent and control for attacks trying to manipulate the training dataset ('data poisoning'), inputs designed to cause the model to make a mistake ('adversarial examples'), or model flaws.

CHAPTER 3

OBLIGATIONS OF PROVIDERS AND USERS 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:

<u>(a)</u> ensure that their high-risk AI systems are compliant with the requirements set out in Chapter 2 of this Title;

Obtenu pour vous par
Got for you by
agence europe

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

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

(c) ~~draw-up~~ **keep** the ~~technical~~ documentation **referred to in Article 18** ~~of the high-risk AI system~~;

(d) when under their control, keep the logs automatically generated by their high-risk AI systems **as referred to in Article 20**;

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

(f) comply with the registration obligations referred to in Article 51**(1)**;

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

(h) inform the **relevant** national competent authorit**y**~~ies~~ 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 their high-risk AI systems to indicate the conformity with this Regulation in accordance with Article 49;

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

Article 17
Quality management system

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

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

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

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

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

   (e) technical specifications, including standards, to be applied and, where the relevant harmonised standards are not applied in full, 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 collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation,

Obtenu pour vous par
Got for you by
agence europe

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 national competent authorities, 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.

2a. For providers of high-risk AI systems that are subject to obligations regarding quality management systems under relevant sectorial Union law, the aspects described in paragraph 1 may be part of the quality management systems pursuant to that law.

3. For providers that are ~~credit~~ **financial** institutions **subject to requirements regarding their internal governance, arrangements or processes under Union financial services legislation** ~~regulated by Directive 2013/36/ EU~~, the obligation to put **in place** a quality management system ~~**in place**~~ **with the exception of paragraph 1, points (g), (h) and (i)** shall be deemed to be fulfilled by complying with the rules on internal governance arrangements **or** processes ~~and mechanisms~~ pursuant to **the relevant Union financial services legislation** ~~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~~ ***Documentation keeping***

1. ~~Providers of high-risk AI systems shall draw up the technical documentation referred to in Article 11 in accordance with Annex IV.~~ **The provider shall, for a period ending 10 years after the AI system has been placed on the market or put into service, keep at the disposal of the national competent authorities:**

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

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

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

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

Obtenu pour vous par
Got for you by
agence europe

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

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

2. Providers that are **financial** ~~credit i~~nstitutions **subject to requirements regarding their internal governance, arrangements or processes under Union financial services legislation** ~~regulated by Directive 2013/36/EU~~ shall maintain the technical documentation as part of the documentation **kept** ~~concerning internal governance, arrangements, processes and mechanisms pursuant to~~ **under the relevant Union financial services legislation** ~~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, **referred to in Article 12(1),** 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. ~~The logs shall be kept~~ **They shall keep them** for a period **of at least six months, unless provided otherwise in** ~~that is appropriate in the light of the intended purpose of high-risk AI system and~~ applicable ~~legal obligations under~~ Union or national law**, in particular in Union law on the protection of personal data**.

2. Providers that are ~~credit~~ **financial** institutions **subject to requirements regarding their internal governance, arrangements or processes under Union financial services legislation** ~~regulated by Directive 2013/36/EU~~ shall maintain the logs automatically generated by their high-risk AI systems as part of the documentation **kept** under **the relevant financial service legislation** ~~Articles 74 of that Directive~~.

Obtenu pour vous par
Got for you by
agence europe

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 investigate, where applicable, the causes in collaboration with the reporting user and** ~~immediately~~ take the necessary corrective actions to bring that system into conformity, to withdraw it or to recall it, as appropriate. They shall inform the distributors of the high-risk AI system in question and, where applicable, the authorised representative and importers accordingly.

Article 22
Duty of information

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, that provider shall immediately inform the national competent 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 of the non-compliance and of any corrective actions taken.

Article 23
Cooperation with competent authorities

Providers of high-risk AI systems shall, upon request by a national competent authority, provide that authority 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 **a language which can be easily understood by the authority of** ~~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, **referred to in Article 12(1)**, 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.

Article 23a
Conditions for other persons to be subject to the obligations of a provider ~~***Obligations of distributors, importers, users or any other third-party***~~

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

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

~~**(b) they modify the intended purpose of a high-risk AI system already placed on the market or put into service;**~~

(c) they make a substantial modification to a high-risk AI system already placed on the market or put into service;

(d) they modify the intended purpose of an AI system which is not high-risk and is already placed on the market or put ito service, in a way which makes the modified system a high-risk AI system;~~.~~

Obtenu pour vous par
Got for you by
agence europe

(e) they place on the market or put into service a general purpose AI system as a high-risk AI system or as a component of a high-risk AI system ~~fulfil the conditions referred in Article 52a(2)~~.

2. Where the circumstances referred to in paragraph 1, point (a) ~~(b)~~ or (c), occur, the provider that initially placed the high-risk AI system on the market or put it into service shall no longer be considered a provider for the purposes of this Regulation.

3. For high-risk AI systems that are safety components of products to which the legal acts listed in Annex II, section A apply, the manufacturer of those products shall be considered the provider of the high-risk AI system and shall be subject to the obligations under Article 16 under either of the following scenarios:

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

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

~~*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.

2. The authorised representative shall perform the tasks specified in the mandate received from the provider. **For the purpose of this Regulation, ~~T~~**the mandate shall empower the authorised representative to carry out **only** the following tasks:

(-a) verify 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;

(a) **keep at the disposal of the national competent authorities and national authorities referred to in Article 63(7), for a period ending 10 years after the high-risk AI system has been placed on the market or put into service, the contact details of the provider by which the authorised representative has been appointed, a copy of the EU declaration of conformity, the technical documentation and, if applicable, the certificate issued by the notified body** ~~keep a copy of the EU declaration of conformity and the technical documentation at the disposal of the national competent authorities and national authorities referred to in Article 63(7)~~;

Obtenu pour vous par
Got for you by
agence europe

(b) provide a national competent authority, upon a reasoned request, with all the information and documentation**, including that kept according to point (b)**, 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**, referred to in Article 12(1)**, automatically generated by the high-risk AI system to the extent such logs are under the control of the provider by virtue of a contractual arrangement with the user or otherwise by law;

(c) cooperate with ~~competent~~ national **competent** authorities, upon a reasoned request, on any action the latter takes in relation to the high-risk AI system.

(d) comply with the registration obligations referred to in Article 51(1) and~~or~~, if the registration of the system is carried out by the provider itself, verify that the information referred to in ~~point 3 of~~ Annex VIII, Part II, 1 to 11, is correct..

The authorised representative shall terminate the mandate if it has sufficient reasons to consider that the provider acts contrary to its obligations under this Regulation. In such a case, it shall also immediately inform the market surveillance 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.

The authorised representative shall be legally liable for defective AI systems on the same basis as, and jointly and severally with, the provider in respect of its potential liability under Council Directive 85/374/EEC.

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 verifying** that:

(a) the ~~appropriate~~ **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 Annex IV;

(c) the system bears the required **CE** conformity marking and is accompanied by **the EU declaration of conformity** and ~~the required documentation and~~ instructions of use~~.~~**;**

(d) the authorised representative referred to in Article 25 has been established by the provider.

2. Where an importer ~~considers or~~ has **sufficient** reason**s** to consider that a high-risk AI system is not in conformity with this Regulation, **or is falsified, or accompanied by falsified documentation,** it shall not place 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, **the authorised representatives** 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 or, where that is not possible, on its packaging or its accompanying documentation, as 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.

Obtenu pour vous par
Got for you by
agence europe

4a. **Importers shall keep, for a period ending 10 years after the AI system has been placed on the market or put into service, a copy of the certificate issued by the notified body, where applicable, of the instructions for use and of the EU declaration of conformity.**

5. Importers shall provide national competent authorities, upon a reasoned request, with all necessary information and documentation**, including that kept in accordance with paragraph 5,** 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 that national competent authority. **To this purpose they shall also ensure that the technical documentation can be made available to those authorities.** ~~, 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. They shall also cooperate with those authorities on any action national competent authority takes in relation to that system.~~

5a. **Importers shall cooperate with national competent authorities on any action those authorities take in relation to an AI system, of which they are the importer.**

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~~ **a copy of EU declaration of conformity and** instruction of use, and that the provider and the importer of the system, as applicable, have complied with the**ir** obligations **set out Article 16, point (b) and 26(3) respectively** ~~in this Regulation~~.

2. Where a distributor considers or has reason to consider 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, 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 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 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 high-risk AI systems shall provide that authority with all the information and documentation **regarding its activities as described in paragraph 1 to 4** ~~necessary to demonstrate the conformity of a high-risk system with the requirements set out in Chapter 2 of this Title~~. ~~Distributors~~

Obtenu pour vous par
Got for you by
agence europe

~~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 in relation to an AI system, of which they are the distributor**.

~~*Article 28*~~

~~*Obligations of distributors, importers, users or any other third-party*~~

~~1. Any distributor, importer, user or other third-party shall be considered a provider **of 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 place on the market or put into service a high-risk AI system under their name or trademark;~~

~~(b) they modify the intended purpose of a high-risk AI system already placed on the market or put into service;~~

~~(c) they make a substantial modification to the high-risk AI system.~~ **~~;~~**

~~(d) they modify the intendent purpose of an AI system which is not high-risk and is already placed on the market or put ito service, in a way which makes the modified system a high-risk AI system.~~

~~2. Where the circumstances referred to in paragraph 1, point (b) or (c), occur, the provider that initially placed the high-risk AI system on the market or put it into service shall no longer be considered a provider for the purposes of this Regulation.~~

Article 29

Obligations of users of high-risk AI systems

1. Users of high-risk AI systems shall use such systems ~~**and implement human oversight**~~ in accordance with the instructions of use accompanying the systems, pursuant to paragraphs 2 and 5 **of this Article**.

1a. **Users shall assign human oversight to natural persons who have the necessary competence, training and authority.**

2. The obligations in paragraph 1 **and 1a** are without prejudice to other user obligations under Union or national law and to the user'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, to the extent the user exercises control over the input data, that user shall ensure that input data is relevant in view of the intended purpose of the high-risk AI system.

4. Users shall **implement human oversight and** monitor the operation of the high-risk AI system on the basis of the instructions of use. 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 inform the provider or distributor and suspend the use of the system. They shall also inform the provider or distributor 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 user is not able to reach the provider, Article 62 shall apply mutatis mutandis. **This obligation shall not cover sensitive operational data of users of AI systems which are law enforcement authorities.**

Obtenu pour vous par
Got for you by
agence europe

For users that are ~~credit~~ **financial** institutions **subject to requirements regarding their internal governance, arrangements or processes under Union financial services legislation** ~~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 the relevant financial service legislation** ~~Article 74 of that Directive~~.

5. Users of high-risk AI systems shall keep the logs**, referred to in Article 12(1),** automatically generated by that high-risk AI system, to the extent such logs are under their control ~~and~~. ~~The logs shall be kept~~ **They shall keep them** for a period **of at least six months, unless provided otherwise**~~ that is appropriate in the light of the intended purpose of the high-risk AI system and~~ **in** applicable~~ legal obligations under~~ Union or national law**, in particular in Union law on the protection of personal data**.

Users that are ~~credit~~ **financial** institutions **subject to requirements regarding their internal governance, arrangements or processes under Union financial services legislation** ~~regulated by Directive 2013/36/EU~~ shall maintain the logs as part of the documentation **kept** ~~concerning internal governance arrangements, processes and mechanisms~~ pursuant to **the relevant Union financial service legislation** ~~Article 74 of that Directive~~.

5a. Users of high-risk AI systems that are public authorities, agencies or bodies, with the exception of law enforcement, border control, immigration or asylum authorities, shall comply with the registration obligations referred to in Article 51. When they find that the system that they envisage to use has not been registered in the EU database referred to in Article 60 they shall not use that system and shall inform the provider or the distributor.

6. Users 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, where applicable.

6a. Users shall cooperate with national competent authorities on any action those authorities take in relation to an AI system, of which they are the user.

~~**7. The obligations established by this Article shall not apply to users who use the high-risk AI system in the course of a personal non-professional activity.**~~

CHAPTER 4

NOTIFIYING AUTHORITIES AND NOTIFIED BODIES

Article 30
Notifying authorities

1. Each Member State shall designate or establish ~~a~~ **at least one** notifying authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring.

Obtenu pour vous par
Got for you by
agence europe

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

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 **in accordance with Article 70**.

7. Notifying authorities shall have ~~a sufficient~~ **an adequate** number of competent personnel at their disposal for the proper performance of their tasks.

8. ~~Notifying authorities shall make sure that conformity assessments are carried out in a proportionate 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.~~

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~~ **AI systems** for which the conformity assessment body claims to be competent, as well as by an accreditation certificate, where one exists, issued by a national accreditation body attesting that the conformity assessment body fulfils the requirements laid down in Article 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 **all** 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. **The notified body shall update the documentation referred to in paragraph 2 and paragraph 3 whenever relevant changes occur, in order to enable the authority responsible for notified bodies to monitor and verify continuous compliance with all the requirements laid down in Article 33.**

Obtenu pour vous par
Got for you by
agence europe

Article 32
Notification procedure

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

2. Notifying authorities shall notify **those bodies to** the Commission and the other Member States using the electronic notification tool developed and managed by the Commission.

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 AI systems concerned** ~~and the artificial intelligence technologies concerned~~ **and the relevant attestation of competence. Where a notification is not based on an accreditation certificate as referred to in Article 31 (2), the notifying authority shall provide the Commission and the other Member States with documentary evidence which attests to the conformity assessment body's competence and the arrangements in place to ensure that that body will be monitored regularly and will continue to satisfy the requirements laid down in Article 33**.

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

~~5. Notifying authorities shall notify the Commission and the other Member States of any subsequent relevant changes to the notification **referred to in this Article without undue delay**.~~

Article 33
Requirements relating to n*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.~~ **A notified body shall be established under national law and have legal personality.**

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

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.

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.

Obtenu pour vous par
Got for you by
agence europe

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 **in accordance with Article 70** 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.

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 **in which they are located** ~~concerned~~ in accordance with national law or that Member State is **itself** 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, t~~**T**he notified body shall have permanent availability of sufficient administrative, technical**, legal** 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 33a
Presumption of conformity with requirements relating to notified bodies

Where a conformity assessment body demonstrates its conformity with the criteria laid down in the relevant harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union it shall be presumed to comply with the requirements set out in Article 33 in so far as the applicable harmonised standards cover those requirements.

Obtenu pour vous par
Got for you by
agence europe

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.

4. ~~Notified bodies shall keep at the disposal of the notifying authority t~~**T**he relevant documents concerning the assessment of the qualifications of the subcontractor or the subsidiary and the work carried out by them under this Regulation **shall be kept at the disposal of the notifying authority for a period of 5 years from the termination date of the subcontracting activity**.

Article 34a

Operational obligations of 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 perform their activities while avoiding unnecessary burdens for providers, and taking due account of the size of an undertaking, the sector in which it operates, its structure and the degree of complexity of the high risk AI system in question. In so doing, the notified body shall nevertheless respect the degree of rigour and the level of protection required for the compliance of the high risk AI system with the requirements of this Regulation.

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

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.

Obtenu pour vous par
Got for you by
agence europe

Article 36
Changes to notifications

1. The notifying authority shall notify the Commission and the other Member States of any relevant changes to the notification of a notified body via the electronic notification tool referred to in Article 32(2).

2. The procedures described in Article 31 and 32 shall apply to extensions of the scope of the notification. For changes to the notification other than extensions of its scope, the procedures laid down in the following paragraphs shall apply.

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

~~1~~**3**. Where a notifying authority has ~~suspicions~~ **sufficient reasons to consider** ~~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, **the notifying authority shall, provided that the the notified body had the opportunity to make its views known, restrict, suspend or withdraw notification as appropriate, depending on the seriousness of the failure to meet those requirements or fulfil those obligations. It shall immediately inform the Commission and the other Member States accordingly** ~~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 authorities**~~ ~~at their request.~~

4. Where its designation has been suspended, restricted, or fully or partially withdrawn, the notified body shall inform the manufacturers concerned at the latest within 10 days.

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

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

Obtenu pour vous par
Got for you by
agence europe

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

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

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

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

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

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

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

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

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

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

b) another notified body has confirmed in writing that it will assume immediate responsibilities for those systems and will have completed assessment of them within twelve months of the withdrawal of the designation.

Obtenu pour vous par
Got for you by
agence europe

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

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

Article 37
Challenge to the competence of notified bodies

1. The Commission shall, where necessary, investigate all cases where there are reasons to doubt whether a notified body complies with the requirements laid down in Article 33.

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

3. The Commission shall ensure that all confidential information obtained in the course of its investigations pursuant to this Article is treated confidentially **in accordance with Article 70.**

4. Where the Commission ascertains that a notified body does not meet or no longer meets the requirements laid down in Article 33, it shall **inform the notifying authority of the reasons of such an ascertainment and request it** ~~adopt a reasoned decision requesting the notifying Member State~~ to take the necessary corrective measures, including ~~withdrawal of~~ ~~**de-**notification~~ **the suspension, restriction or withdrawal of the designation** if necessary. ~~That implementing act shall be adopted in accordance with the examination procedure referred to in Article 74(2).~~ **Where the notifying authority fails to take the necessary corrective measures, the Commission may, by means of implementing acts, suspend, restrict or withdraw the notification. 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~~ **high-risk AI systems**, 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~~ **The notifying authority** shall ensure that the bodies notified by them participate in the work of that group, directly or by means of designated representatives.

Article 39
Conformity assessment bodies of third countries

Conformity assessment bodies established under the law of a third country with which the Union has concluded an agreement may be authorised to carry out the activities of notified Bodies under this Regulation**, provided that they meet the requirements in Article 33**.

Obtenu pour vous par
Got for you by
agence europe

CHAPTER 5

STANDARDS, CONFORMITY ASSESSMENT, CERTIFICATES, REGISTRATION

Article 40
Harmonised standards

1. High-risk AI systems **or general purpose AI systems** which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements set out in Chapter 2 of this Title **or, as applicable, with requirements set out in Article 4a and Article 4b**, to the extent those standards cover those requirements.

2. When issuing a standardisation request to European standardisation organisations in accordance with Article 10 of Regulation 1025/2012, the Commission shall specify that standards are coherent, clear ~~easy to implement~~ and drafted in such a way that they aim to fulfil in particular the following objectives:

a) ensure that AI systems placed on the market or put into service in the Union are safe and respect Union values and strengthen the Union's digital sovereignty open strategic autonomy;

b) promote investment and innovation in AI, including through increasing legal certainty, as well as competitiveness and growth of the Union market;

c) enhance multistakeholder governance, representative of all relevant European stakeholders (e.g. industry, SMEs, civil society, researchers).

d) contribute to strengthening global cooperation on standardisation in the field of AI that is consistent with Union values and interests.

The Commission shall request the European standardisation organisations to provide evidence of their best efforts to fulfil the above objectives.

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, **after consulting the AI Board referred to in Article 56**, by means of implementing acts, adopt common specifications in respect of the requirements set out in Chapter 2 of this Title **or, as applicable, with requirements set out in Article 4a and Article 4b**. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74(2).~~

1. The Commission is empowered to adopt, after consulting the AI Board referred to in Article 56, implementing acts <u>in accordance with the examination procedure referred to in Article 74(2)</u> establishing common technical specifications for the requirements set out in Chapter 2 of this Title, or, as applicable, with requirements set out in Article 4a and Article 4b, where the following conditions have been fulfilled:

Obtenu pour vous par
Got for you by
agence europe

(a) no reference to harmonised standards covering the relevant essential safety or fundamental right concerns is published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012;

(b) the Commission has requested, pursuant to Article 10(1) of Regulation 1025/2012, one or more European standardisation organisations to draft a harmonised standard for the requirements set out in Chapter 2 of this Title;

(c) the request referred to in point(b) has not been accepted by any of the European standardisation organisations ~~or the standard is not delivered within the deadline~~ or the harmonised standards addressing that request are not delivered within the deadline set in accordance with article 10(1) of Regulation 1025/2012 or those standards do not comply with the request.

1a. Before preparing a draft implementing act, the Commission shall inform the committee referred to in Article 22 of Regulation EU (No) 1025/2012 that it considers that the conditions in paragraph 1 are fulfilled.

2. **In the early preparation of the draft implementing act establishing the common specification, the Commission shall fulfil the objectives referred to in Article 40(2) and gather the views of relevant bodies or expert groups established under relevant sectorial Union law. Based on that consultation, the Commission shall prepare the draft implementing act.**

~~The Commission, **W**when preparing the common specifications referred to in paragraph 1, **the Commission** shall **fulfil the objectives referred of Article 40(2) and** gather the views of relevant bodies or expert groups established under relevant sectorial Union law.~~

3. High-risk AI systems **or general purpose AI systems** which are in conformity with the common specifications referred to in paragraph 1 shall be presumed to be in conformity with the requirements set out in Chapter 2 of this Title **or, as applicable, with requirements set out in Article 4a and Article 4b**, to the extent those common specifications cover those requirements.

4. When references of a harmonised standard are published in the Official Journal of the European Union, implementing acts referred to in paragraph 1, which cover the requirements set out in Chapter 2 of this Title or requirements set out in Article 4a and Article 4b, shall be repealed, as applicable.

5. When a Member State considers that a common specification does not entirely satisfy the requirements set out in Chapter 2 of this Title or requirements set out in Article 4a and Article 4b, as applicable, it shall inform the Commission thereof with a detailed explanation and the Commission shall assess that information and, if appropriate, amend the implementing act establishing the common specification in question.

~~4. Where providers do not comply with the common specifications referred to in paragraph 1, they shall duly justify **in the technical documentation referred to in Article 11** that they have adopted technical solutions that are at least equivalent thereto.~~

Article 42
Presumption of conformity with certain requirements

1. ~~Taking into account their intended purpose, h~~**H**igh-risk AI systems that have been trained and tested on data ~~concerning~~ **reflecting** the specific geographical, behavioural ~~and~~ **or**

Obtenu pour vous par
Got for you by
agence europe

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 **or general purpose 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[34] 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 ~~follow~~ **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.

   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 not applied or has applied only in part harmonised standards referred to in Article 40, or where such harmonised standards do not exist and common specifications referred to in Article 41 are not available, the provider shall follow the conformity assessment procedure set out in Annex VII.

   For the purpose of 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 2 to 8 of Annex III **and for general purpose AI systems referred in Title 1a**, 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

[34] 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).

Obtenu pour vous par
Got for you by
agence europe

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 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 user.~~

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

5. The Commission is empowered to adopt delegated acts in accordance with Article 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.

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.

Article 44
Certificates

1. Certificates issued by notified bodies in accordance with Annex VII shall be drawn-up in a~~n~~ ~~official~~ ~~Union~~ **a** language ~~determined~~ **which can be easily undestood** by **the relevant authorities in** the Member State in which the notified body is established ~~or in an official Union language otherwise acceptable to the notified body~~.

2. Certificates shall be valid for the period they indicate, which shall not exceed five years. On application by the provider, the validity of a certificate may be extended for further periods, each not exceeding five years, based on a re-assessment in accordance with the applicable conformity assessment procedures. **Any supplement to a certificate shall remain valid as long as the certificate which it supplements is valid.**

3. Where a notified body finds that an AI system no longer meets the requirements set out in Chapter 2 of this Title, it shall, taking account of the principle of proportionality, suspend

Obtenu pour vous par
Got for you by
agence europe

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~~ ~~a~~**A**n appeal procedure against decisions of the notified bodies ~~is~~ **shall be** 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~~ **AI systems** with relevant information on issues relating to negative and, on request, positive conformity assessment results.

4. The obligations referred to in paragraphs 1 to 3 shall be complied with in accordance with Article 70.

Article 47
Derogation from conformity assessment procedure

1. By way of derogation from Article 43 **and upon a duly justified request**, any market surveillance authority may authorise the placing on the market or 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,

Obtenu pour vous par
Got for you by
agence europe

environmental protection and the protection of key industrial and infrastructural assets. That authorisation shall be for a limited period of time **while the necessary conformity assessment procedures are being carried out**, **taking into account the exceptional reasons justifying the derogation.**~~, 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.

1a. In a duly justified situation of urgency for exceptional reasons of public security or in case of specific, substantial and imminent threat to the life or physical safety of natural persons, law enforcement authorities or civil protection authorities may put a specific high-risk AI system into service without the authorisation referred to in paragraph 1 provided that such authorisation is requested during or after the use without undue delay, and if such authorisation is rejected, its use shall be stopped with immediate effect.

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

~~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 of an authorisation issued by a market surveillance authority of a Member State in accordance with paragraph 1, that authorisation shall be deemed justified.~~

~~4. Where, within 15 calendar days of receipt of the notification referred to in paragraph 2, objections are raised by a Member State against an authorisation issued by a market surveillance authority of another Member State, or where the Commission considers the authorisation to be contrary to Union law 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; 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 or operators.~~

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

6. ~~By way of derogation from paragraphs 1 to 5,f~~**F**or high-risk AI systems ~~*intended to be used as safety components of* devices~~ **related to products**~~, or which are themselves devices,~~ covered by **Union harmonisation legislation referred to in Annex II Section A, only the conformity assessment derogation procedures established in that legislation shall apply.** ~~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.~~.

Obtenu pour vous par
Got for you by
agence europe

Article 48
EU declaration of conformity

1. The provider shall draw up a written **or electronically signed** EU declaration of conformity for each AI system and keep it at the disposal of the national competent authorities for 10 years after the AI system has been placed on the market or put into service. The EU declaration of conformity shall identify the AI system for which it has been drawn up. A copy of the EU declaration of conformity shall be ~~given~~ **submitted** to 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~~ **a** language~~s~~ **that can be easily understood by the national competent authorities of** ~~required by~~ the Member State(s) in which the high-risk AI system is made available.

3. Where high-risk AI systems are subject to other Union harmonisation legislation which also requires an EU declaration of conformity, a single EU declaration of conformity shall be drawn up in respect of all Union 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. 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 CE marking of conformity** ~~**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.** ~~The CE marking shall be affixed visibly, legibly and indelibly for high-risk AI systems. Where that is not possible or not warranted on account of the nature of the high-risk AI system, it shall be affixed to the packaging or to the accompanying documentation, as appropriate.~~

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

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 shall also be indicated in any promotional material which mentions that the high-risk AI system fulfils the requirements for CE marking.

Obtenu pour vous par
Got for you by
agence europe

~~*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 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 ***of relevant operators and of high-risk AI systems listed in Annex III***

1. Before placing on the market or putting into service a high-risk AI system listed in Annex III ~~referred to in Article 6(3),~~ **with the exception of high-risk AI systems referred to in Annex III, points 1, 6 and 7 in the areas of law enforcement, migration, asylum and border control management, and high risk AI systems referred to in Annex III point 2,** the provider **and** ~~or,~~ where applicable, the authorised representative shall register **themselves** ~~that system~~ in the EU database referred to in Article 60. **The provider or, where applicable the authorised representative, shall also register their systems in that database.**

2. Before using a high-risk AI system listed in Annex III, users of high-risk AI systems that are public authorities, agencies or bodies, with the exception of law enforcement, border control, immigration or asylum authorities and authorities using high-risk AI systems referred to Annex III point 2, shall register themselves in the EU database referred to in Article 60 and select the system that they envisage to use.

TITLE IV

TRANSPARENCY OBLIGATIONS FOR PROVIDERS AND USERS OF CERTAIN AI SYSTEMS

Article 52
Transparency obligations for ***providers and users of*** *certain AI systems*

1. Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way ~~**that those systems inform**~~ ~~*that*~~ **that** natural persons ~~are informed~~ **are informed** that they are interacting with an AI system, unless this is obvious **from the point of view of a** ~~**reasonable**~~ **natural person who is reasonably well-informed, observant and circumspect, taking into account** ~~from~~ the circumstances and the context of use. This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences, **subject to appropriate safeguards for the rights and freedoms of third parties,** unless those systems are available for the public to report a criminal offence.

2. Users of ~~an emotion recognition system or~~ a biometric categorisation system shall inform of the operation of the system the natural persons exposed thereto. This obligation shall not apply to AI systems used for biometric categorisation, which are permitted by law to

Obtenu pour vous par
Got for you by
agence europe

detect, prevent and investigate criminal offences**, subject to appropriate safeguards for the rights and freedoms of third parties**.

2a. **Users of an emotion recognition system shall inform of the operation of the system the natural persons exposed thereto. This obligation shall not apply to AI systems used for emotion recognition which are permitted by law to detect, prevent and investigate criminal offences, subject to appropriate safeguards for the rights and freedoms of third parties.** ~~**in the context of criminal investigations**~~**.**

3. Users of an AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ('deep fake'), shall disclose that the content has been artificially generated or manipulated.

However, the first subparagraph shall not apply where the use is authorised by law to detect, prevent, investigate and prosecute criminal offences **or where the content is part of an evidently creative, satirical, artistic or fictional work or programme** ~~or it is necessary for the exercise of the right to freedom of expression and the right to freedom of the arts and sciences guaranteed in the Charter of Fundamental Rights of the EU, and~~ subject to appropriate safeguards for the rights and freedoms of third parties.

3a. **The information referred to in paragraphs 1 to 3 shall be provided to natural persons in a clear and** ~~**visible**~~ **distinguishable manner at the latest at the time of the first interaction or exposure.**

4. Paragraphs 1, 2**, 2a and 3** and 3**a** shall not affect the requirements and obligations set out in Title III of this Regulation~~.~~ **and shall be without prejudice to other transparency obligations for users of AI systems laid down in Union or national law**.

~~TITLE IVA~~

~~GENERAL PURPOSE AI SYSTEMS~~

~~*Article 52a*~~

~~*General purpose AI systems*~~

~~**1. The placing on the market, putting into service or use of general purpose AI systems shall not, by themselves only, make those systems subject to the provisions of this Regulation.**~~

~~**2. Any person who places on the market or puts into service under its own name or trademark or uses a general purpose AI system made available on the market or put into service for an intended purpose that makes it subject to the provisions of this Regulation shall be considered the provider of the AI system subject to the provisions of this Regulation.**~~

~~**3. Paragraph 2 shall apply, mutatis mutandis, to any person who integrates a general purpose AI system made available on the market, with or without modifying it, into an AI system whose intended purpose makes it subject to the provisions of this Regulation.**~~

Obtenu pour vous par
Got for you by
agence europe

~~**4. The provisions of this Article shall apply irrespective of whether the general purpose AI system is open source software or not.**~~

TITLE V

MEASURES IN SUPPORT OF INNOVATION

Article 53
AI regulatory sandboxes

-1a. National competent authorities may establish AI regulatory sandboxes for the development, training, testing and validation of innovative AI systems under the direct supervision, guidance and support by the national competent authority, before those systems are ~~cir~~ place~~dment~~ on the market or put~~ting~~ into service. Such regulatory sandboxes may include testing in real world conditions supervised by the national competent authorities.

~~**-1b. In relation to AI systems provided by the EU institutions, bodies and agencies, such AI regulatory sandboxes may be established by the European Data Protection Supervisor.**~~

-1c Where appropriate, national competent authorities shall cooperate with other relevant ~~national~~ authorities and may allow for the involvement of other actors within the AI ecosystem ~~such as national or European standardisation organisations, notified bodies, testing and experimentation facilities, research and experimentation labs and innovation hubs~~.

-1d. This Article ~~Paragraphs -1a and -1b~~ shall not affect other regulatory sandboxes established under national or Union law~~.~~, including in cases where the products or services that are tested in them are linked to the use of innovative AI systems. Member States shall ensure an appropriate level of cooperation between the authorities supervising those other sandboxes and the national competent authorities.

1. ~~AI regulatory sandboxes established by one or more Member States competent authorities or the European Data Protection Supervisor shall provide a controlled environment that facilitates the~~**~~for 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. This shall take place under the direct supervision and guidance by the~~ **~~national~~** ~~competent authorities~~ **~~and, where appropriate, in cooperation with other relevant national authorities, or by the European Data Protection Supervisor in relation to AI systems provided by the EU institutions, bodies and agencies.~~** ~~with a view to ensuring compliance with the requirements of this Regulation and, where relevant, other Union and Member States legislation supervised within the sandbox.~~

~~**1a. The national competent authority or the European Data Protection Supervisor, as appropriate, may also supervise testing in real world conditions upon the request of participants in the sandbox.**~~

1b. The establishment of AI regulatory sandboxes under this Regulation ~~as defined in paragraph 1~~ shall aim to contribute to one or more of the following objectives:

Obtenu pour vous par
Got for you by
agence europe

a) foster innovation and competitiveness and facilitate the development of an AI ecosystem;

b) facilitate and accelerate access to the Union market for AI systems, ~~including~~ in particular when provided by small and medium enterprises (SMEs), including ~~and~~ start-ups;

c) improve legal certainty and contribute to the sharing of best practices through cooperation with the authorities involved in the AI regulatory sandbox with a view to ensuring future compliance with this Regulation and, where appropriate, with other Union and Member States legislation;

d) contribute to evidence-based regulatory learning;

~~e) enhance authorities' understanding of the opportunities and risks of AI systems as well as of the suitability and effectiveness of the measures for preventing and mitigating those risks;~~

~~f) contribute to the uniform and effective implementation of this Regulation and, where appropriate, its swift adaptation, notably as regards the techniques in Annex I, the high-risk AI systems in Annex III, the technical documentation in Annex IV;~~

~~g) contribute to the development or update of harmonised standards and common specifications referred to in Articles 40 and 41 and their uptake by providers.~~

2. **~~The AI regulatory sandboxes may be established upon the decision of the national competent authorities, including jointly with those from other Member States, or by the European Data Protection Supervisor. They may be established upon request of any provider or prospective provider having an interest in participating in the sandbox, or at the sole initiative of the national competent authorities or the European Data Protection Supervisor.~~**

~~Member States shall ensure that to the extent the innovative AI systems involve the processing of personal data or otherwise fall under the supervisory remit of other national authorities or competent authorities providing or supporting access to data, the national data protection authorities and those other national authorities are associated to the operation of the AI regulatory sandbox.~~

~~As appropriate, national competent authorities may allow for the involvement in the AI regulatory sandbox of other actors within the AI ecosystem such as national or European standardisation organisations, notified bodies, testing and experimentation facilities, research and experimentation labs and innovation hubs~~.

2a. ~~Access to the AI regulatory sandboxes and supervision and guidance by the relevant authorities shall be free of charge, without prejudice to exceptional costs that national competent authorities may recover in a fair and proportionate manner. It~~ Access to the AI regulatory sandboxes shall be open to any provider or prospective provider of an AI system who fulfils the eligibility and selection criteria referred to in paragraph 6(a) and who has been selected by the national competent authorities ~~or, where applicable, by the European Data Protection Supervisor~~ following the selection procedure referred to in paragraph 6(b). Providers or prospective providers may also submit applications in partnership with users or any other relevant third parties.

Participation in the AI regulatory sandbox shall be limited to a period that is appropriate to the complexity and scale of the project ~~in any case not longer than a maximum period of 2 years, starting upon the notification of the selection decision.~~

Obtenu pour vous par
Got for you by
agence europe

~~**The participation may be extended for up to 1 more year**~~**. This period may be extended by the national competent authority.**

Participation in the AI regulatory sandbox shall be based on a specific plan referred to in paragraph 6 of this Article that shall be agreed between the participant(s) and the national competent authoritie(s) ~~**or the European Data Protection Supervisor**~~**, as applicable.** ~~**The plan shall contain as a minimum the following:**~~

~~**a) description of the participant(s) involved and their roles, the envisaged AI system and its intended purpose, and relevant development, testing and validation process;**~~

~~**b) the specific regulatory issues at stake and the guidance that is expected from the authorities supervising the AI regulatory sandbox;**~~

~~**c) the specific modalities of the collaboration between the participant(s) and the authoritie(s), as well as any other actor involved in the AI regulatory sandbox;**~~

~~**d) a risk management and monitoring mechanism to identify, prevent and mitigate any risk referred to in Article 9(2)(a);**~~

e) ~~**the key milestones to be completed by the participant(s) for the AI system to be considered ready to exit from the regulatory sandbox.**~~

3. The **participation in the** AI regulatory sandboxes shall not affect the supervisory and corrective powers of the ~~competent~~ authorities **supervising the sandbox**. **Those authorities shall exercice their supervisory powers in a flexible manner within the limits of the relevant legislation, using their discretionary powers when implementing legal provisions to a specific AI sandbox project**~~.~~**, with the objective of supporting innovation in AI in the Union** ~~Any significant risks to health and safety and fundamental rights identified during the development and testing of such systems shall result in immediate mitigation and, failing that, in the suspension of the development and testing process until such mitigation takes place.~~

~~**However, p**~~**Provided that the participant(s) respect the sandbox plan and the terms and conditions for their participation as referred to in paragraph 6(c) and follow in good faith the guidance given by the authorities, no administrative** ~~**enforcement action shall be taken**~~ **fines shall be imposed by the authorities for infringement of applicable Union or Member State legislation** **relating to the AI system supervised in the sandbox**, **including the provisions of this Regulation.**

4. **The p**~~P~~articipants ~~in the AI regulatory sandbox~~ remain liable under applicable Union and Member States liability legislation for any ~~harm~~ **damage caused** ~~inflicted~~ ~~on third parties~~ **in the course of their participation** ~~as a result from the experimentation taking place~~ in ~~the~~ **an AI-regulatory** sandbox.

4a. Upon request of the provider or prospective provider of the AI system, the national competent authority shall provide, where applicable, a written proof of the activities successfully carried out in the sandbox. The national competent authority ~~**may**~~ **shall also provide an exit report detailing the activities carried out in the sandbox and the related** **results and learning** **outcomes. Such written proof and exit report could be taken into account by market surveillance authorities or notified bodies, as applicable, in the context of conformity assessment procedures or market surveillance checks.**

Subject to the confidentiality provisions in Article 70 and with the agreement of the sandbox participants, the European Commission and the AI Board shall be authorised to access the exit reports and shall take them into account, as appropriate,

Obtenu pour vous par
Got for you by
agence europe

when exercising their tasks under this Regulation. If both the participant and the national competent authority explicitly agree to this, the exit report can be made publicly available through the single information platform referred to in article 55(3)(b).

4b. **The AI regulatory sandboxes shall be designed and implemented in such a way that, where relevant, they facilitate cross-border cooperation between the national competent authorities.** ~~**and synergies with relevant sectoral regulatory sandboxes. Cooperation may also be envisaged with third countries outside the Union establishing mechanisms to support AI innovation.**~~

5. ~~Member States'~~ ~~**National**~~ ~~competent authorities that have established AI regulatory sandboxes~~ ~~**and the European Data Protection Supervisor**~~ ~~shall coordinate their activities and cooperate within the framework of the European Artificial Intelligence Board.~~

~~They~~ **National competent authorities shall make publicly available** ~~**publish on their websites**~~ ~~submit~~ annual reports **on** ~~to the Board and the Commission~~ on ~~the results from~~ the implementation of ~~those~~ **the AI regulatory sandboxes**, including good practices, lessons learnt and recommendations on their setup and, where relevant, on the application of this Regulation and other Union legislation supervised within the sandbox. **Those annual reports shall be submitted to the AI Board which shall make publicly available** ~~**publish on its website**~~ **a summary of all good practices, lessons learnt and recommendations**. **This obligation to make annual reports publicly available shall not cover sensitive operational data in relation to the activities of law enforcement, border control, immigration or asylum authorities. The Commission and the AI Board shall, where appropriate, take the annual reports into account when exercising their tasks under this Regulation.**

5b. **The Commission shall ensure that information about AI regulatory sandboxes, including about those established under this Article, is available through** ~~**a**~~ **the single information platform** ~~**as**~~ **referred to in Article 55(3)(b).**

6. The ~~**detailed**~~ modalities and the conditions **for the establishment and** ~~of the~~ operation of the AI regulatory sandboxes **under this Regulation**~~, 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 shall be set out in implementing acts. Those implementing acts~~ shall be adopted **through implementing acts** in accordance with the examination procedure referred to in Article 74(2).

The modalities and conditions shall to the best extent possible support flexibility for national competent authorities to establish and operate their AI regulatory sandboxes, foster innovation and regulatory learning and shall particularly take into account the special circumstances and capacities of participating SMEs, including start-ups.

Those implementing acts shall include ~~**general common rules**~~ **common main principles on the following issues:**

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

b) ~~**the**~~ **procedure for the application,** ~~**selection,**~~ **participation, monitoring,** ~~**and**~~ **exiting from and termination of the AI regulatory sandbox, including the sandbox plan and the exit report** ~~**including templates of all relevant documents**~~**;**

Obtenu pour vous par
Got for you by
agence europe

c) the terms and conditions applicable to the participants~~, including in relation to their collaboration with the authorities supervising the sandbox, as well as the conditions for suspension and termination of the participation in the sandbox~~;

~~**d) the modalities for the involvement in the AI regulatory sandbox of other national authorities and other actors within the AI ecosystem;**~~

~~**e) the modalities and procedures for cross-border cooperation, including the establishment and operation by two or more Member States of cross-border AI regulatory sandboxes.**~~

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

Article 54

*~~Further~~ ~~p~~ **Further p~~P~~**rocessing 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** ~~lawfully collected for other purposes~~ ~~shall~~ **may** be processed for the purposes of developing**,** ~~and~~ testing **and training of** ~~certain~~ innovative AI systems in the sandbox under the following **cumulative** conditions:

(a) the innovative AI systems shall be developed for safeguarding substantial public interest **by a public authority or another natural or legal person governed by public law or by private law and** 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~~ prevention, control and treatment **of disease and improvement of health care systems**;

(iii) ~~a high level of~~ protection and improvement of the quality of the environment**, including green transition, climate change mitigation and adaptation;**

(iv) energy sustainability, transport and mobility;

(v) ~~a high level of~~ efficiency and quality of public administration and public services~~.~~;

(vi) cybersecurity and resilience of critical infrastructure.

(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;

Obtenu pour vous par
Got for you by
agence europe

(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~~39 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 participants and only authorised persons have access to that data;

(e) any personal data processed are not **to** be transmitted, transferred or otherwise accessed by other parties **that are not participants in the sandbox, unless such disclosure occurs in compliance with ~~the GDPR~~ Regulation (EU) 2016/679 or, where applicable, Regulation 2018/725, and all participants have agreed to it ~~nor transferred to a third country outside the Union or an international organisation~~**;

(f) any processing of personal data in the context of the sandbox ~~do not lead to measures or decisions affecting the data subjects~~; **shall not affect the application of the rights of the data subjects as provided for under Union law on the protection of personal data, in particular in Article 22 of Regulation (EU) 2016/679 and Article 24 of Regulation (EU) 2018/1725;**

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

(h) the logs of the processing of personal data in the context of the sandbox are kept for the duration of the participation in the sandbox**, unless provided otherwise by Union or national law** ~~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 project developed in the sandbox, its objectives and expected results published on the website of the competent authorities. **This obligation shall not cover sensitive operational data in relation to the activities of law enforcement, border control, immigration or asylum authorities.**

1a. For the purpose of 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 law enforcement authorities, the processing of personal data in AI regulatory sandboxes shall be based on a specific Member State or Union law and subject to the same cumulative conditions as referred to in paragraph 1.

2. ~~Paragraph 1 is without prejudice to Union or Member States legislation excluding processing for other purposes than those explicitly mentioned in that legislation.~~ **Paragraph 1 is without prejudice to Union or Member States laws laying down the basis for the processing of personal data which is necessary for the purpose of**

Obtenu pour vous par
Got for you by
agence europe

developing, testing and training of innovative AI systems or any other legal basis, in compliance with Union law on the protection of personal data.

Article 54a

Testing of high-risk AI systems in real world conditions outside AI regulatory sandboxes

1. Testing of AI systems in real world conditions outside AI regulatory sandboxes may be conducted by providers or prospective providers of high-risk AI systems listed in Annex III, in accordance with the provisions of this Article and the real-world testing plan referred to in this Article.

The detailed elements of the real-world testing plan shall be specified in implementing acts adopted by the Commission in accordance with the examination procedure referred to in Article 74(2).

This provision shall be without prejudice to Union or Member State legislation for the testing in real world conditions of high-risk AI systems related to products covered by legislation listed in Annex II.

2. Providers or prospective providers may conduct testing of high-risk AI systems referred to in Annex III in real world conditions at any time before the placing on the market or putting into service of the AI system on their own or in partnership with one or more prospective users.

~~The testing in real world conditions under this Article may occur in the course of the participation in a AI regulatory sandbox under the conditions specified in Article 53(1a). In such a case, supervision and guidance by the national competent authorities or, where applicable, the European Data Protection Supervisor, may be extended to the testing in real world conditions.~~

3. The testing of high-risk AI systems in real world conditions under this Article shall be without prejudice to ethical review that may be required by national or Union law.

4. Providers or prospective providers may conduct the testing in real world conditions only where all of the following conditions are met:

(a) the provider or prospective provider has drawn up a real-world testing plan and submitted it to the market surveillance authority in the Member State(s) where the testing in real world conditions is to be conducted ~~or the European Data Protection Supervisor, as applicable~~;

(b) the market surveillance authority in the Member State(s) where the testing in real world conditions is to be conducted ~~or to the European Data Protection Supervisor~~, ~~as applicable~~, have not objected to the testing within 30 days after its submission;

(c) the provider or prospective provider with the exception of high-risk AI systems referred to in Annex III, points 1, 6 and 7 in the areas of law enforcement, migration, asylum and border control management, and high risk AI systems referred to in Annex III point 2, has registered the testing in real world conditions in the EU database referred to in Article ~~60(6)~~ 60(5a) with a Union-wide unique single identification number and the information specified in Annex VIIIa;

(d) the provider or prospective provider conducting the testing in real world conditions is established in the Union or it has appointed a legal representative for the purpose of the testing in real world conditions who is established in the Union;

Obtenu pour vous par
Got for you by
agence europe

(e) data collected and processed for the purpose of the testing in real world conditions shall not be transferred to countries outside the Union, unless the transfer and the processing provides equivalent safeguards to those provided under Union law;

(f) the testing in real world conditions does not last longer than necessary to achieve its objectives and in any case not longer than 12 months;

~~**(g) the testing in real world conditions does not involves persons belonging to vulnerable groups due to their age, physical or mental disability, only when such testing does not exploit any of those vulnerabilities unless that testing is essential with respect to those vulnerable groups insofar as data of comparable validity cannot be obtained through testing in real conditions on other persons or by other methods;**~~ **persons belonging to vulnerable groups due to their age, physical or mental disability are appropriately protected;**

~~**(h) the testing in real world conditions is designed to involve as little inconvenience as possible for the subjects of that testing; such possible inconvenience shall be specifically anticipated and defined by the provider or prospective provider in the real-world testing plan, monitored and possibly mitigated in the course of the testing;**~~

(i) where a provider or prospective provider organises the testing in real world conditions in cooperation with one or more prospective users, the latter have been informed of all aspects of the testing that are relevant to their decision to participate, ~~including~~ and given the relevant instructions on how to ~~of~~ use ~~of~~ the AI system referred to in Article 13; the provider or prospective provider and the user(s) shall conclude an agreement specifying their roles and responsibilities with a view to ensuring compliance with the provisions for testing in real world conditions under this Regulation and other applicable Union and Member States legislation;

(j) the subjects of the testing in real world conditions have given informed consent in accordance with Article 54~~64~~b, or in the case of law enforcement, where the seeking of informed consent would prevent the AI system from being tested, the testing itself and the outcome of the testing in the real world conditions shall not have a negative effect on the subject;

(k) the testing in real world conditions is effectively overseen by the provider or prospective provider and user(s) with persons who are suitably qualified in the relevant field and have the necessary capacity, training and authority to perform their tasks;

(l) the predictions, recommendations or decisions of the AI system can be effectively reversed or disregarded.

5. Any subject of the testing in real world conditions, or his or her legally designated representative, as appropriate, may, without any resulting detriment and without having to provide any justification, withdraw from the testing at any time by revoking his or her informed consent. The withdrawal of the informed consent shall not affect the activities already carried out and the use of data obtained based on the informed consent before its withdrawal.

6. Any serious incident ~~or malfunctioning~~ identified in the course of the testing in real world conditions shall be reported to the national market surveillance authority in accordance with Article 62 of this Regulation. The provider or prospective provider shall adopt immediate mitigation measures or, failing that, suspend the testing in real world conditions until such mitigation takes place or otherwise terminate it. The

Obtenu pour vous par
Got for you by
agence europe

provider or prospective provider shall establish a procedure for the prompt recall of the AI system upon such termination of the testing in real world conditions.

7. Providers or prospective providers shall notify the national market surveillance authority in the Member State(s) where the testing in real world conditions is to be conducted ~~or the European Data Protection Supervisor, as applicable~~, of the suspension or termination of the testing in real world conditions and the final outcomes.

8. The provider and prospective provider shall be liable under applicable Union and Member States liability legislation for any damage caused ~~to the subjects~~ ~~by reason~~ in the course of their participation in the testing in real world conditions.

Article 54b

Informed consent to participate in testing in real world conditions outside AI regulatory sandboxes

1. For the purpose of testing in real world conditions under Article 54a, informed consent shall be freely given by the subject of testing prior to his or her participation in such testing and after having been duly informed with concise, clear, relevant, and understandable information regarding:

(i) the nature and objectives of the testing in real world conditions and the possible inconvenience that may be linked to his or her participation;

(ii) the conditions under which the testing in real world conditions is to be conducted, including the expected duration of the subject's participation;

(iii) the subject's rights and guarantees regarding participation, in particular his or her right to refuse to participate in and the right to withdraw from testing in real world conditions ~~the field testing~~ at any time without any resulting detriment and without having to provide any justification;

(iv) the modalities for requesting the reversal or the disregard of the predictions, recommendations or decisions of the AI system;

(v) the Union-wide unique single identification number of the testing in real world conditions in accordance with ~~Article 54a(c)~~ Article 54a(4c) and the contact details of the provider or its legal representative from whom further information can be obtained.

2. The informed consent shall be dated and documented and a copy shall be given to the subject or his or her legal representative.

Article 55

Support m~~M~~easures for operators, in particular SMEs, including start-ups ~~small-scale providers and users~~

1. Member States shall undertake the following actions:

(a) provide ~~small-scale~~ SME**s** ~~providers~~**, including** ~~and~~ start-ups**,** with priority access to the AI regulatory sandboxes to the extent that they fulfil the eligibility ~~conditions~~ **and selection criteria**;

Obtenu pour vous par
Got for you by
agence europe

(b) organise specific awareness raising **and training** activities about the application of this Regulation tailored to the needs of the ~~small-scale~~ **SMEs** ~~providers and users~~**, including start-ups, and, as appropriate, local public authorities**;

(c) where appropriate, establish a dedicated channel for communication with ~~small-scale~~ **SMEs** ~~providers and user~~**, including start-ups**~~,~~ **and, as appropriate, local public authorities** ~~and other innovators~~ to provide ~~guidance~~ **advice** and respond to queries about the implementation of this Regulation~~.~~**, including as regards participation in AI regulatory sandboxes.**

2. The specific interests and needs of the ~~small-scale~~ **SME** providers**, including start-ups,** shall be taken into account when setting the fees for conformity assessment under Article 43, reducing those fees proportionately to their size**,** ~~and~~ market size **and other relevant indicators**.

3. The Commission shall undertake the following actions:

(a) **upon request of the AI Board, provide standardised** ~~**documents**~~ **templates for the areas covered by this Regulation;**

(b) **develop and maintain a single information platform providing easy to use information in relation to this Regulation for all operators across the Union;**

(c) **organise appropriate communication campaigns to raise awareness about the obligations arising from this Regulation;**

(d) **evaluate and promote the convergence of best practices in public procurement procedures in relation to AI systems.**

Obtenu pour vous par
Got for you by
agence europe

Article 55a

Derogations for specific operators

1. The obligations laid down in Article 17 of this Regulation shall not apply to microenterprises as defined in Article 2(3) of the Annex to the Commission Recommendation 2003/361/EC concerning the definition of micro, small and medium-sized enterprises, provided those enterprises do not have partner enterprises or linked enterprises as defined in Article 3 of the same Annex.

2. Paragraph 1 shall not be interpreted as exempting those operators from fulfilling any other requirements and obligations laid down in this Regulation, including those established in Articles 9, 61 and 62.

3. Requirements and obligations for general purpose AI systems laid down in Article 4b shall not apply to micro, small and medium-sized enterprises, provided those enterprises do not have partner enterprises or linked enterprises as defined in Article 3 of the the Annex to the Commission Recommendation 2003/361/EC concerning the definition of micro, small and medium-sized enterprises.

TITLE VI

GOVERNANCE

CHAPTER 1

EUROPEAN ARTIFICIAL INTELLIGENCE BOARD

Article 56
*Establishment **and structure** of the European Artificial Intelligence Board*

1. A 'European Artificial Intelligence Board' (the 'Board') is established.

~~2. The Board shall provide advice and assistance to the Commission in order to:~~

~~(a) contribute to the effective cooperation of the national supervisory authorities and the Commission with regard to matters covered by this Regulation;~~

~~(b) coordinate and contribute to guidance and analysis by the Commission and the national supervisory authorities and other competent authorities on emerging issues across the internal market with regard to matters covered by this Regulation;~~

~~(c) assist the national supervisory authorities and the Commission in ensuring the consistent application of this Regulation.~~

Obtenu pour vous par
Got for you by
agence europe

~~*Article 57*~~
~~*Structure of the Board*~~

~~1~~**2**. The Board shall be composed of **one representative per Member State** ~~the national supervisory authorities, who shall be represented by the head or equivalent high-level official of that authority,~~ ~~**and of eight independent experts representing SMEs and start-ups, large enterprises, academia and civil society, in equal proportions of 2 members per category.**~~ ~~and~~ ~~t~~**T**he European Data Protection Supervisor **shall participate as an observer**. **The Commission shall also attend the Board's meetings without taking part in the votes.**

Other national **and Union** authorities**, bodies or experts** may be invited to the meetings **by the Board on a case by case basis**, where the issues discussed are of relevance for them.

2a. Each representative shall be designated by their Member State for a period of 3 years, renewable once. ~~**The eight independent experts referred to paragraph 2 shall be selected by the Member States national representatives in a fair and transparent selection process established in the Board's rules of procedure, for a period of 3 years, renewable once.**~~

2aa. Member States shall ensure that their representatives in the Board:

(i) have the relevant competences and powers in their Member State so as to contribute actively to the achievement of the board's tasks referred to in Article 58;

(ii) are designated as a single contact point vis-à-vis the Board and, where appropriate, taking into account Member States' needs, as a single contact point for stakeholders;

(iii) are empowered to facilitate consistency and coordination between national competent authorities in their Member State as regards the implementation of this Regulation, including through the collection of relevant data and information for the purpose of fulfilling their tasks on the Board.

~~2~~**3**. The ~~Board~~ **designated representatives of the Member States** shall adopt ~~its~~ **the Board's** rules of procedure by a ~~simple~~ **two-thirds** majority ~~of its members, following the consent of the Commission~~. ~~The rules of procedure shall also contain the operational aspects related to the execution of the Board's tasks as listed in Article 58.~~

The rules of procedure shall, in particular, lay down procedures for ~~**the selection process for the eight independent experts referred to in paragraph 1, as well as**~~ **the selection process, duration of mandate and specifications of the tasks of the Chair, the voting modalities, and the organisation of the Board's activities and its sub-groups.**

The Board shall establish a standing subgroup serving as a platform for stakeholders to advise the Board on all issues related to the implementation of this Regulation, including on the preparation of implementing and delegated acts. To this purpose, organisations representing the interests of the providers and users of AI systems, including SMEs and start-ups, as well as civil society organisations, representatives of affected persons, researchers, standardisation organisations, notified bodies, laboratories and testing and experimentation facilities shall be invited to participate to this sub-group. The Board shall establish two standing sub-groups to provide a platform for cooperation and exchange among market surveillance authorities and notifying authorities on issues related to market surveillance and notified bodies respectively.

Obtenu pour vous par
Got for you by
agence europe

The Board may establish **other standing or temporary** sub-groups as appropriate for the purpose of examining specific ~~questions~~ **issues**. **Where appropriate, ~~organisations representing the interests of the providers and users of AI systems, including SMEs and start-ups, as well as civil society organisations, representatives of affected persons, researchers, standardisation organisations, notified bodies, laboratories and testing and experimentation facilities~~ stakeholders referred to in the previous subparagraph may be invited to such sub-groups or to specific meetings of those subgroups in the capacity of observers.**

3a. **The Board shall be organised and operated so as to safeguard the objectivity and impartiality of its activities.**

~~3~~**4**. The Board shall be chaired by **one of the representatives of the Member States.** ~~the Commission~~. **Upon request of the Chair,** ~~T~~the Commission shall convene the meetings and prepare the agenda in accordance with the tasks of the Board pursuant to this Regulation and ~~with~~ its rules of procedure. The Commission shall provide administrative and analytical support for the activities of the Board pursuant to this Regulation.

~~45. The Board may invite external experts and observers to attend its meetings and may hold exchanges with interested third parties to inform its activities to an appropriate extent. To that end the Commission may facilitate exchanges between the Board and other Union bodies, offices, agencies and advisory groups.~~

Article 58
Tasks of the Board

~~When providing advice and assistance to the Commission in the context of Article 56(2),~~ **The Board shall advice and assist the Commission and the Member States in order to facilitate the consistent and effective application of this Regulation. For this purpose** the Board **may** ~~shall~~ in particular:

(a) collect and share **technical and regulatory** expertise and best practices among Member States;

(b) contribute to ~~uniform~~ **the harmonisation of** administrative practices in the Member States, including **in relation to** ~~for~~ **the derogation from the conformity assessment procedures referred to in Article 47,** the functioning of regulatory sandboxes and **testing in real world conditions** referred to in Article 53**, 54 and 54a**;

(c) **upon the request of the Commission or on its own initiative,** issue ~~opinions, recommendations or~~ **recommendations and** written **opinions** ~~contributions~~ **on any relevant** matters related to the implementation of this Regulation **and to its consistent and effective application**, **including:** ~~in particular~~

(i) on technical specifications or existing standards regarding the requirements set out in Title III, Chapter 2,

(ii) on the use of harmonised standards or common specifications referred to in Articles 40 and 41,

(iii) on the preparation of guidance documents, including the guidelines concerning the setting of administrative fines referred to in Article 71~~.~~**;**

(d) ~~**issue an advisory opinion on the need for amendment of Annex I and Annex III, including in light of available evidence.**~~ **advise the Commission on the potential need for**

Obtenu pour vous par
Got for you by
agence europe

amendment of Annex~~es I and~~ III in accordance with Articles 4 and 7, taking into account relevant available evidence and the latest develoments in technology;

(e) advise the Commission during the preparation of delegated or implementing act pursuant to this Regulation;

f) cooperate, as appropriate, with relevant EU bodies, experts groups and networks in particular in the fields of product safety, cybersecurity, competition, digital and media services, financial services, cryptocurrencies, consumer protection, data and fundamental rights protection;

g) contribute and provide relevant advice to the Commission in the development of the guidance referred to in Article 58a or request the development of such guidance;

(h) to assist the work of market surveillance authorities and, in cooperation and subject to agreement of the concerned market surveillance authorities, promote and support cross-border market surveillance investigations~~;~~, notably with respect to the emergence of risks of systemic nature that may stem from AI systems;

(i) contribute to the assessment of training needs for staff of Member States involved in implementing this Regulation;

(j) advise the Commission in relation to international matters on artificial intelligence.

CHAPTER 1A

GUIDELINES FROM THE COMMISSION

Article 58a
Guidelines from the Commission on the implementation of this Regulation

1. Upon the request of the Member States or the Board, or on its own initiative, the Commission shall issue guidelines on the practical implementation of this Regulation, and in particular on

(i) the application of the requirements referred to in Articles 8 - 15;

(ii) the prohibited practices referred to in Article 5;

(iii) the practical implementation of the provisions related to substantial modification;

(iv) the practical implementation of uniform conditions referred to in Article 6, paragraph 3, including examples ~~identification and application of criteria and~~ in relation to ~~use cases related~~ high risk AI systems referred to in Annex III;

(v) the practical implementation of transparency obligations laid down in Article 52;

(vi) the relationship of this Regulation with other relevant Union legislation.

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.

Obtenu pour vous par
Got for you by
agence europe

CHAPTER 2

NATIONAL COMPETENT AUTHORITIES

Article 59
Designation of national competent authorities

~~1. National competent authorities shall be established or designated by each Member State for the purpose of ensuring the application and implementation of this Regulation. National competent authorities shall be organised so as to safeguard the objectivity and impartiality of their activities and tasks.~~

2. Each Member State shall **establish or** designate ~~a national supervisory authority~~**, and at least one notifying authority and at least one market surveillance authority for the purpose of this Regulation as** ~~among the~~ national competent authorities. **These national competent authorities shall be organised so as to safeguard the priniciples of objectivity and impartiality of their activities and tasks. Provided that those prinicples are respected, such activities and tasks may be performed by one or several designated authorities, in accordance with the organisational needs of the Member State.** ~~The national supervisory authority shall act as notifying authority and market surveillance authority unless a Member State has organisational and administrative reasons to designate more than one authority.~~

3. Member States shall inform the Commission of their designation or designations ~~and, where applicable, the reasons for designating more than one authority~~.

4. Member States shall ensure that national competent authorities are provided with adequate financial **resources, technical equipment and well qualified** ~~and~~ human resources to **effectively** fulfil their tasks under this Regulation. ~~In particular, national competent authorities 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, fundamental rights, health and safety risks and knowledge of existing standards and legal requirements.~~

5. **By *[one year after entry into force of this Regulation]* and afterwards six months before the deadline referred to in Article 84(2)** Member States shall ~~report to~~ **inform** the Commission ~~on an annual basis~~ on the status of the financial **resources, technical equipment and** ~~and~~ human resources of the national competent authorities with an assessment of their adequacy. The Commission shall transmit that information to the Board for discussion and possible recommendations.

6. The Commission shall facilitate the exchange of experience between national competent authorities.

7. National competent authorities may provide ~~guidance and~~ advice on the implementation of this Regulation, including **tailored** to ~~small-scale~~ **SME** providers**, including start-ups**. Whenever national competent authorities intend to provide guidance and advice with regard to an AI system in areas covered by other Union legislation, the competent national authorities under that Union legislation shall be consulted, 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.

Obtenu pour vous par
Got for you by
agence europe

TITLE VII

EU DATABASE FOR ~~STAND-ALONE~~ HIGH-RISK AI SYSTEMS LISTED IN ANNEX III

Article 60
EU database for ~~stand-alone~~ high-risk AI systems ***listed in Annex III***

1. The Commission shall, in collaboration with the Member States, set up and maintain a EU database containing information referred to in paragraph 2 concerning **relevant operators and** high-risk AI systems **listed in Annex III** ~~referred to in Article 6(2)~~ which are registered in accordance with Articles 51 **and 54a**. **When setting the fuctional specifications of such database, the Commission shall consult the AI Board.**

2. **The data listed in Annex VIII, Part I, shall be entered into the EU database by the providers, authorised representatives and relevant users, as applicable, upon their registration.** The data listed in Annex VIII**, Part II, 1 to 11,** shall be entered into the EU database by the providers, **or where applicable by the authorised representative, in accordance with Article 51. The data referred in Annex VIII, Part II, 12 shall be automatically generated by the database based on the information provided by <u>relevant</u> users pursuant to Article 51(2). The data listed in Annex VIIIa shall be entered into the database by the prospective providers or providers in accordance with Article 54a**. ~~The Commission shall provide them with technical and administrative support.~~

3. ~~Information contained in the EU database shall be accessible to the public~~.

4. The EU database shall contain **no** personal data**, except for the information listed in Annex VIII<u>, and shall be without prejudice to Article 70</u>** ~~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~~.

5. The Commission shall be the controller of the EU database. It shall ~~also~~ ~~**ensure**~~ **make available** to providers**,** ~~**and**~~ **prospective providers and users** adequate technical and administrative support.

5a. Information contained in the EU database registered in accordance with Article 51 shall be accessible to the public. The information registered in accordance with Article 54a shall be accessible only to market surveillance authorites and the Commission, unless the prospective provider or provider has given consent for making this information also accessible the public.

Obtenu pour vous par
Got for you by
agence europe

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. **In order to allow the provider to evaluate the compliance of AI systems with the requirements set out in Title III, Chapter 2 throughout their life cycle,** ~~T~~the post-market monitoring system shall ~~actively and systematically~~ collect, document and analyse relevant data**, which may be** provided by users or **which may be** collected through other sources on the performance of high-risk AI systems**. This obligation shall not cover sensitive operational data of users of AI systems which are law enforcement authorities.** ~~throughout their life time and allow the provider to evaluate the continuous compliance of AI systems with the requirements set out in Title III, Chapter 2.~~

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.

4. For high-risk AI systems covered by the legal acts referred to in Annex II, **Section A,** 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 post-market monitoring documentation as prepared under that legislation shall be deemed sufficient, provided that the template referred to paragraph 3 is used**.

   The first subparagraph shall also apply high-risk AI systems referred to in point 5~~(b)~~ of Annex III placed on the market or put into service by ~~credit~~ **financial** institutions **that are subject to requirements regarding their internal governance, arrangements or processes under Union financial services legislation.**~~regulated by Directive 2013/36/EU~~.

Obtenu pour vous par
Got for you by
agence europe

CHAPTER 2

SHARING OF INFORMATION ON SERIOUS INCIDENTS ~~AND MALFUNCTIONING~~

Article 62
Reporting of serious incidents ~~and of malfunctioning~~

1. Providers 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 market surveillance authorities of the Member States where that incident ~~or breach~~ occurred.

   Such notification shall be made immediately after the provider has established a causal link between the AI system and the **serious** incident ~~or malfunctioning~~ or the reasonable likelihood of such a link, and, in any event, not later than 15 days after the providers becomes aware of the serious incident ~~or of the malfunctioning~~.

2. Upon receiving a notification related to a **serious incident referred to in Article 3(44)(c)** ~~a breach of obligations under Union law intended to protect fundamental rights~~, the **relevant** market surveillance 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 12 months after the entry into force of this Regulation, at the latest.

3. For high-risk AI systems referred to in point 5~~(b)~~ of Annex III which are placed on the market or put into service by providers that are ~~credit~~ **financial** institutions **that are subject to requirements regarding their internal governance, arrangements or processes under Union financial services legislation** ~~regulated by Directive 2013/36/EU and for high-risk AI systems which are safety components of devices, or are themselves devices, covered by Regulation (EU) 2017/745 and Regulation (EU) 2017/746~~, the notification of serious incidents ~~or malfunctioning~~ shall be limited to those **referred to in Article 3(44)(c)**~~that that constitute a breach of obligations under Union law intended to protect fundamental rights~~.

4. **For high-risk AI systems which are safety components of devices, or are themselves devices, covered by Regulation (EU) 2017/745 and Regulation (EU) 2017/746 the notification of serious incidents shall be limited to those referred to in Article 3(44)(c) and be made to the national ~~supervisory~~ competent authority chosen for this purpose by ~~of~~ the Member States where that incident occurred.**

Obtenu pour vous par
Got for you by
agence europe

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 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~~ **Article 2** of this Regulation;

   (b) any reference to a product under Regulation (EU) 2019/1020 shall be understood as including all AI systems falling within the scope of this Regulation.

2. **As part of their reporting obligations under Article ~~25(6)~~ 34(4) of Regulation (EU) 2019/1020, the ~~Member States~~ market surveillance authorities** ~~national supervisory authority~~ shall report to the Commission ~~on a regular basis~~ **about** the outcomes of relevant market surveillance activities **under this Regulation**. ~~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 **or, in justified circumstances and provided that coordination is ensured, another relevant authority identified by the Member State.**

   The procedures referred to in Articles 65, 66, 67 and 68 of this Regulation shall not apply to AI systems related to products, to which legal acts listed in Annex II, section A apply, when such legal acts already provide for procedures having the same objective. In such a case, these sectoral procedures shall apply instead.

4. For **high-risk** 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 **national** authority responsible for the financial supervision of those institutions under that legislation~~.~~ **in so far as the placement on the market, putting into service or the use of the AI system is in direct connection with the provision of those financial services.**

   By way of a derogation from the previous subparagraph, ~~When the placement on the market, putting into service or the use of the AI system is not in direct connection with the provision of financial services, or~~ in justified circumstances and provided that coordination is ensured, another relevant authority may be identified by the Member State as market surveillance authority for the purposes of this Regulation.

   National market surveillance authorities supervising regulated credit institutions regulated under Directive 2013/36/EU, which are participating in the Single Supervisory Mechanism (SSM) established by Council Regulation No 1204/2013, should report, without delay, to the European Central Bank any information identified in the course of their market surveillance activities that may be of potential interest for the European Central Bank's prudential supervisory tasks as specified in

Obtenu pour vous par
Got for you by
agence europe

that Regulation ~~Council Regulation (EU) No 1204/2013 establishing the Single Supervisory Mechanism (SSM)~~.

5. For **high-risk** AI systems listed in point 1(a) in so far as the systems are used for law enforcement purposes, points 6~~, and~~ 7 and 8 of Annex III, Member States shall designate as market surveillance authorities for the purposes of this Regulation either **the national authorities supervising the activities of the law enforcement, border control, immigration, ~~or~~ asylum or judicial authorities** ~~systems~~, or 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 those systems~~. **Market surveillance activities shall in no way affect the independence of judicial authorities or otherwise interfere with their activities when acting in their judicial capacity.**

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. Member States shall facilitate the coordination between market surveillance authorities designated under this Regulation and other relevant national authorities or bodies which supervise the application of 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.

8. Without prejudice to powers provided under Regulation (EU) 2019/1020, and where relevant and limited to what is necessary to fulfil their tasks, the market surveillance authorities shall be granted full access by the provider to the documentation as well as the training, validation and testing datasets used for the development of the high-risk AI system, including, where appropriate and subject to security safeguards, through application programming interfaces ('API') or other relevant technical means and tools enabling remote access.

9. Market surveillance authorities shall be granted access to the source code of the high-risk AI system upon a reasoned request and only when the following cumulative conditions are fulfilled:

a) Access to source code is necessary to assess the conformity of a high-risk AI system with the requirements set out in Title III, Chapter 2, and

b) testing/auditing procedures and verifications based on the data and documentation provided by the provider have been exhausted or proved insufficient.

10. Any information and documentation obtained by market surveillance authorities shall be treated in compliance with the confidentiality obligations set out in Article 70.

11. Complaints to the relevant market surveillance authority can be submitted by a~~A~~ny natural or legal person having grounds to consider that there has been an infringement of the provisions ~~a high-risk AI system is not in compliance with the requirements~~ of this Regulation ~~shall be entitled to submit a complaint to the relevant market surveillance authority.~~

In accordance with Article 11(3)(e) and (7)(a) of Regulation (EU) 2019/1020, complaints shall be taken into account for the purpose of conducting the market surveillance activities and be handled in line with the dedicated procedures established therefore by the market surveillance authorities.

Obtenu pour vous par
Got for you by
agence europe

Article 63a

Supervision of testing in real world conditions by market surveillance authorities

1. Market surveillance authorities shall have the competence and powers to ensure that testing in real world conditions is in accordance with this Regulation.

2. Where testing in real world conditions is conducted for AI systems that are supervised within an AI regulatory sandbox under Article 54, the market surveillance authorities ~~or the European Data protection Supervisor, as appropriate,~~ shall verify the compliance with the provisions of Article 54a as part of their supervisory role for the AI regulatory sandbox. Those authorities may, as appropriate, allow the testing in real world conditions to be conducted by the provider or prospective provider in derogation to the conditions set out in Article 54a(4) (f) and (g).

3. Where a market surveillance authority has been informed by the prospective provider, the provider or any third party of a serious incident or has other grounds for considering that the conditions set out in Articles 54a and 54b are not met, it may take any of the following decisions on its territory, as appropriate:

(a) suspend or terminate the testing in real world conditions;

(b) require the provider or prospective provider and user(s) to modify any aspect of the testing in real world conditions.

4. Where a market surveillance authority has taken a decision referred to in paragraph 3 of this Article or has issued an objection within the meaning of Article 54a(4)(b), the decision or the objection shall indicate the grounds thereof and the modalities and conditions for the provider or prospective provider to challenge the decision or objection.

5. Where applicable, where a market surveillance authority has taken a decision referred to in paragraph 3 of this Article, it shall communicate the grounds therefor to the market surveillance authorities of the other Member States in which the AI system has been tested in accordance with the testing plan.

Article 64

Powers of authorities protecting fundamental rights ~~*Access to data and documentation*~~

~~1. Access to data and documentation in the context of their activities, the market surveillance authorities shall be granted full access to the training, validation and testing datasets used by the provider, including 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 and upon a reasoned request, the market surveillance authorities shall be granted access to the source code of the AI system.~~

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 market surveillance authority of the Member State concerned of any such request.

Obtenu pour vous par
Got for you by
agence europe

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~~ **the** list publicly available ~~on the website of the national supervisory authority~~. Member States shall notify the list to the Commission and all other Member States and keep the list up to date.

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 paragraph 3 may make a reasoned request to the market surveillance authority to organise testing of the high-risk AI system through technical means. The market surveillance authority shall organise the testing with the close involvement of the requesting public authority or body within 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 a product presenting a risk defined in Article 3, point 19 of Regulation (EU) 2019/1020 insofar as risks to the health or safety or to ~~the protection of~~ fundamental rights of persons are concerned.

2. Where the market surveillance authority of a Member State has sufficient reasons to consider that an AI system presents a risk as referred to in paragraph 1, they 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 **identified** ~~present~~, the market surveillance authority shall also inform the relevant national public authorities or bodies referred to in Article 64(3). The relevant operators shall cooperate as necessary with the market surveillance authorities and the other national public authorities or bodies referred to in Article 64(3).

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

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

3. Where the market surveillance authority considers that non-compliance is not restricted to its national territory, it shall inform the Commission and the other Member States **without undue delay** of the results of the evaluation and of the actions which it has required the operator to take.

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

Obtenu pour vous par
Got for you by
agence europe

appropriate provisional measures to prohibit or restrict the AI system's being made available on its national market, to withdraw the product from that market or to recall it. That authority shall ~~inform~~ **notify** the Commission and the other Member States, without **undue** delay, of those measures.

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

(-a) non-compliance with the prohibition of the artificial intelligence practices referred to in Article 5;

(a) a failure of **a high-risk** AI system to meet requirements set out in Title III, Chapter 2;

(b) shortcomings in the harmonised standards or common specifications referred to in Articles 40 and 41 conferring a presumption of conformity.

(c) non-compliance with provisions set out in Article 52;

(d) non-compliance of general purpose AI systems with the requirements and obligations referred to in Article 4a;

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

8. Where, within three months of receipt of the ~~information~~ **notification** referred to in paragraph 5, no objection has been raised by either a Member State or the Commission in respect of a provisional measure taken by a Member State, that measure shall be deemed justified. 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 market surveillance authorities of all Member States shall **then** ensure that appropriate restrictive measures are taken in respect of the ~~product~~ **AI system** concerned, such as withdrawal of the product from their market, without **undue** delay.

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 a Member State against a measure taken by another Member State, or where the Commission considers the measure to be contrary to Union law, the Commission shall without **undue** delay enter into consultation with the relevant Member State**'s market surveillance authority** and

Obtenu pour vous par
Got for you by
agence europe

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 9 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). **It shall** and notify such decision to the Member State concerned. **The Commission shall also inform all other Member States of such decision.**

2. If the ~~national~~ **measure taken by the relevant Member State's market surveillance authority** is considered justified **by the Commission, the market surveillance 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 undue delay,** ~~shall take the measures necessary to ensure that the non-compliant AI system is withdrawn from their market,~~ and shall inform the Commission accordingly. If the national measure is considered unjustified **by the Commission, the market surveillance authority of** the Member State concerned shall withdraw the measure **and inform the Commission accordingly**.

3. Where the national measure is considered justified and the non-compliance of the AI system is attributed to shortcomings in the harmonised standards or common specifications referred to in Articles 40 and 41 of this Regulation, the Commission shall apply the procedure provided for in Article 11 of Regulation (EU) No 1025/2012.

Article 67

*Compliant **high-risk or general purpose** AI systems which present a risk*

1. Where, having performed an evaluation under Article 65, the market surveillance authority of a Member State finds that although a~~n~~ **high-risk or general purpose** AI system is in compliance with this Regulation, it presents a risk to the health or safety of persons~~,~~ **or** to ~~the compliance with obligations under Union or national law intended to protect~~ fundamental rights ~~or to other aspects of public interest protection~~, it shall require the relevant operator to take all appropriate measures to ensure that the AI system concerned, when placed on the market or put into service, no longer presents that risk, to withdraw the AI system from the market or to recall it **without undue delay** ~~within a reasonable period, commensurate with the nature of the risk~~, **within a period** 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 market surveillance authority of the Member State referred to in paragraph 1.

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

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

5. The Commission shall address its decision to the Member States **concerned, and inform all other Member States**.

Obtenu pour vous par
Got for you by
agence europe

Article 68
Formal non-compliance

1. Where the market surveillance authority of a Member State makes one of the following findings, it shall require the relevant provider to put an end to the non-compliance concerned, **within a period it may prescribe**:

   (a) the conformity marking has been affixed in violation of Article 49;

   (b) the conformity marking has not been affixed;

   (c) the EU declaration of conformity has not been drawn up;

   (d) the EU declaration of conformity has not been drawn up correctly;

   (e) the identification number of the notified body, which is involved in the conformity assessment procedure, where applicable, has not been affixed;

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

Article 68a
Union testing facilities in the area of artificial intelligence

1. The Commission shall designate one or more Union testing facilities pursuant to Article 21 of Regulation (EU) 1020/2019 in the area of artificial intelligence.

2. Without prejudice to the activities of Union testing facilities referred to in Article 21(6) of Regulation (EU) 1020/2019, Union testing facilities referred to in paragraph 1 shall also provide independent technical or scientific advice at the request of the Board or market surveillance authorities.

Article 68b
Central pool of independent experts

1. Upon request of the AI Board, t~~T~~he Commission shall ~~may~~, by means of an implementing act, make provisions on the creation, maintenance and financing of a central pool of independent experts to support the enforcement activities under this Regulation.

2. Experts shall be selected by the Commission and included in the central pool on the basis of up-to-date scientific or technical expertise in the field of artificial intelligence, having due regard to the technical areas covered by the requirements and obligations in this Regulation and the activities of market surveillance authorities pursuant to Article 11 of Regulation (EU) 1020/2019. The Commission shall determine the number of experts in the pool in accordance with the required needs.

3. Experts may have the following tasks:

(a) provide advice to and support the work of market surveillance authorities, at their request;

(b) support cross-border market surveillance investigations as referred to in Article 58(h), without prejudice of the powers of market surveillance authorities;

Obtenu pour vous par
Got for you by
agence europe

(c) advise and support the Commission when carrying out its duties in the context of the safeguard clause pursuant to Article 66.

4. The experts shall perform their tasks with impartiality, objectivity and ensure the confidentiality of information and data obtained in carrying out their tasks and activities. Each expert shall draw up a declaration of interests, which shall be made publicly available. The Commission shall establish systems and procedures to actively manage and prevent potential conflicts of interest.

5. The Member States may be required to pay fees for the advice and support by the experts. The structure and the level of fees as well as the scale and structure of recoverable costs shall be adopted by the Commission by means of the implementing act referred to in paragraph 1, taking into account the objectives of the adequate implementation of this Regulation, cost-effectiveness and the necessity to ensure an effective access to experts by all Member States.

6. The Commission shall facilitate timely access to the experts by the Member States, as needed, and ensure that the combination of support activities carried out by Union testing facilities pursuant to Article ~~70~~ 68a and experts pursuant to this Article is efficiently organised and provides the best possible added value.

TITLE IX

CODES OF CONDUCT

Article 69

*Codes of conduct **for voluntary application of specific requirements***

1. The Commission, and the Member States shall ~~encourage and~~ facilitate the drawing up of codes of conduct intended to ~~foster~~ **encourage** the voluntary application to AI systems other than high-risk AI systems **of one or more of** the requirements set out in Title III, Chapter 2 **of this Regulation to the best extent possible**, **taking into account the available, technical solutions allowing for the application of such requirements.** ~~on the basis of technical specifications and solutions that are appropriate means of ensuring compliance with such requirements in light of the intended purpose of the systems.~~

2. The Commission and the ~~Board~~ **Member States** shall ~~encourage and~~ facilitate the drawing up of codes of conduct intended to **encourage** ~~foster~~ the voluntary application to **all** AI systems of **specific** requirements related**,** for example**,** to environmental sustainability, **including as regards energy-efficient programming,** accessibility for persons with a disability, stakeholders participation in the design and development of the AI systems and diversity of development teams on the basis of clear objectives and key performance indicators to measure the achievement of those objectives. **The Commission and the Member States shall also facilitate, where appropriate, the drawing of codes of conduct applicable on a voluntary basis with regard to users' obligations in relation to AI systems.**

3. Codes of conduct **applicable on a voluntary basis** may be drawn up by individual providers of AI systems or by organisations representing them or by both, including with the involvement of users and any interested stakeholders and their representative organisations, **or, where appropriate, by users with regard to their obligations**. Codes

Obtenu pour vous par
Got for you by
agence europe

of conduct may cover one or more AI systems taking into account the similarity of the intended purpose of the relevant systems.

4. The Commission and the ~~Board~~ **Member States** shall take into account the specific interests and needs of ~~the small-scale~~ **SME** providers, including ~~and~~ start-ups**,** when encouraging and facilitating the drawing up of codes of conduct **referred to in this Article**.

TITLE X

CONFIDENTIALITY AND PENALTIES

Article 70
Confidentiality

1. National competent authorities**,** ~~and~~ notified bodies**, the Commission, the Board, and any other natural or legal person** involved in the application of this Regulation shall**, in accordance with Union or national law, put appropriate technical and organisational measures in place to ensure** ~~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, 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;

(c) public and national security interests;

~~(c)~~ **(d)** integrity of criminal or administrative proceedings~~.~~**;**

(e) the integrity of information classified in accordance with Union or national law.

2. Without prejudice to paragraph 1, information exchanged on a confidential basis between the national competent authorities and between national competent authorities and the Commission shall not be disclosed without the prior consultation of the originating national competent authority and the user when high-risk AI systems referred to in points 1, 6 and 7 of Annex III are used by law enforcement**, border control,** immigration or asylum authorities, when such disclosure would jeopardise public and national security interests. **This obligation to exchange information shall not cover sensitive operational data in relation to the activities of law enforcement, border control, immigration or asylum authorities.**

When the law enforcement, immigration or asylum authorities are providers of high-risk AI systems referred to in 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.

3. Paragraphs 1 and 2 shall not affect the rights and obligations of the Commission, Member States **and their relevant authorities, as well as** ~~and~~ notified bodies**,** with regard to the exchange of information and the dissemination of warnings**, including in the context of**

Obtenu pour vous par
Got for you by
agence europe

cross-border cooperation, nor the obligations of the parties concerned to provide information under criminal law of the Member States.

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 and shall take all measures necessary to ensure that they are properly and effectively implemented. The penalties provided for shall be effective, proportionate, and dissuasive. They shall take into particular account the **size and** interests of ~~small-scale~~ **SME** providers**, including** ~~and~~ start-ups**,** and their economic viability. **They shall also take into account whether the use of the AI system is in the context of personal non-professional activity.**

2. The Member States shall **without delay** notify the Commission of those rules and of those measures and ~~shall notify it, without delay,~~ of any subsequent amendment affecting them.

3. ~~The following infringements~~ **Non-compliance with any of the prohibitions of the artificial intelligence practices referred to in Article 5** shall be subject to administrative fines of up to 30 000 000 EUR or, if the offender is company, up to 6 % of its total worldwide annual turnover for the preceding financial year, ~~whichever is higher~~ **whichever is higher.** ~~**and**~~ **In case of SMEs, including** ~~**and**~~ **start-ups, these fines shall be up to 3% of their** ~~**its**~~ **worldwide annual turnover for the preceding financial year**~~**, whichever is higher**~~**.**~~:~~

   ~~(a) non-compliance with the prohibition of the artificial intelligence practices referred to in Article 5;~~

   ~~(b) non-compliance of the AI system with the requirements laid down in Article 10.~~

4. ~~The~~ **Infringements of the following provisions** ~~non-compliance of the AI system with any requirements or obligations under this Regulation~~ ~~**on**~~ **related to operators or notified bodies**, ~~other than those laid down in Articles 5 and 10~~, 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 higher~~ **whichever is higher**~~**. and In case of SMEs, and including start-ups, these fines shall be up to 2% 3% of their its worldwide annual turnover for the preceding financial year, whichever is higher**~~.

   -a) obligations of providers pursuant to Article 4b;

   a) obligations of providers pursuant to Article 16;

   b) obligations for certain other persons pursuant to Article 23a;

   c) obligations of authorised representatives pursuant to Article 25;

   d) obligations of importers pursuant to Article 26;

   e) obligations of distributors pursuant to Article 27;

   f) obligations of users pursuant to Article 29, paragraphs 1 to 6a;

   g) requirements and obligations of notified bodies pursuant to Article 33, 34(1), 34(3), 34(4), 34a;~~;~~

   h) transparency obligations for providers and users pursuant to Article 52.

Obtenu pour vous par
Got for you by
agence europe

**In case of SMEs, ~~and~~ including start-ups, these fines shall be up to 2% ~~3%~~ of their ~~its~~ 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 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~~ **whichever is higher. ~~and~~ In case of SMEs, ~~and~~ including start-ups, these fines shall be up to 1% ~~3%~~ of their ~~its~~ worldwide annual turnover for the preceding financial year~~, whichever is higher~~.**

6. 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;

(aa) the intentional or negligent character of the infringement;

(ab) any action taken by the operator in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(b) whether administrative fines have been already applied by other market surveillance authorities **in other Member States** to the same operator for the same infringement;

(ba) whether administrative fines have been already applied by other authorities to the same operator for infringements of other Union or national law, when such infringements result from the same activity or omission constituting a relevant infringement of this Act;

(c) the size**, the annual turnover** and market share of the operator committing the infringement;

(d) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

7. Each Member State shall lay down rules on whether and to what extent administrative fines may 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~~ **or** other bodies as applicable in those Member States. The application of such rules in those Member States shall have an equivalent effect.

9. The exercise by the market surveillance authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective 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:

Obtenu pour vous par
Got for you by
agence europe

(a) the nature, gravity and duration of the infringement and of its consequences;

(b) the 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;

2. ~~The following infringements~~ **Non-compliance with any of the prohibitions of the artificial intelligence practices referred to in Article 5** shall be subject to administrative fines of up to 500 000 EUR~~.:~~

~~(a) non-compliance with the prohibition of the artificial intelligence practices referred to in Article 5;~~

~~(b) non-compliance of the AI system with the requirements laid down in Article 10.~~

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 250 000 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 be the income of the general budget of the Union.

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 delegation of power referred to in ~~Article 4,~~ Article 7(1), **Article 7(3),** Article 11(3), Article 43(5) and (6) and Article 48(5) shall be conferred on the Commission for ~~an~~ **a** ~~indeterminate~~ period of ~~time~~ **five years** from [*entering into force of the Regulation*].

The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the 5 year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European

Obtenu pour vous par
Got for you by
agence europe

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 7(3),** 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.

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 7(3),** 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

Obtenu pour vous par
Got for you by
agence europe

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

Obtenu pour vous par
Got for you by
agence europe

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.

_____

* 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.”.

Obtenu pour vous par
Got for you by
agence europe

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

1. This Regulation shall not apply to 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 before *[12 months after the date of application of this Regulation referred to in Article 85(2)]*, unless the replacement or amendment of those legal acts leads to a significant change in the design or intended purpose of the AI system or AI systems concerned.

   The requirements laid down in this Regulation shall be taken into account, where applicable, 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.

2. This Regulation shall apply to the 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 significant changes in their design or intended purpose.

~~**3. Without prejudice to paragraphs 1 and 2, high-risk AI systems that have been placed on the market before [*date of application of this Regulation referred to in Article 85(2)*], may continue to be made available on the market until 3 years after [date of application of this Regulation referred to in Article 85(2)].**~~

Article 84
Evaluation and review

~~1. The Commission shall assess the need for amendment of the list in Annex III once a year following the entry into force of this Regulation.~~

~~**1a. The Commission shall assess the need for amendment of the list in Annex I every 24 months following the entry into force of this Regulation and until the end of the period of the delegation of power. The findings of that assessment shall be presented to the European Parliament and the Council.**~~

1b. The Commission shall assess the need for amendment of the list in Annex III every 24 months following the entry into force of this Regulation and until the end of the period of the delegation of power. The findings of that assessment shall be presented to the European Parliament and the Council.

2. By [*three years after the date of application of this Regulation referred to in Article 85(2)*] and every four years thereafter, the Commission shall submit a report on the evaluation and

Obtenu pour vous par
Got for you by
agence europe

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 **resources, technical equipment and** ~~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.

4**.** Within [*three years after the date of application of this Regulation referred to in Article 85(2)*] and every four years thereafter**, where appropriate**, the Commission shall evaluate the impact and effectiveness of **voluntary** codes of conduct to foster the application of the requirements set out in Title III, Chapter 2 **for AI systems other than high-risk AI systems** and possibly other additional requirements for AI systems ~~other than high-risk AI systems.~~**, including as regards environmental sustainability.**

5. For the purpose of paragraphs 1**a** to 4 the Board, the Member States and national competent authorities shall provide the Commission with information on its request.

6. In carrying out the evaluations and reviews referred to in paragraphs 1**a** to 4 the Commission shall take into account the positions and findings of the Board, of the European Parliament, of the Council, and of other relevant bodies or sources.

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

Article 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~~ **36** 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~~ **twelve** 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.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

Obtenu pour vous par
Got for you by
agence europe

~~**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.~~

Obtenu pour vous par
Got for you by
agence europe

ANNEX II
LIST OF UNION HARMONISATION LEGISLATION
Section A – List of Union harmonisation legislation based on the New Legislative Framework

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

Obtenu pour vous par
Got for you by
agence europe

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).

Obtenu pour vous par
Got for you by
agence europe

Section B. List of other Union harmonisation legislation

1. 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).

2. 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);

3. 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);

4. 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);

5. 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).

6. 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);

7. 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);

Obtenu pour vous par
Got for you by
agence europe

8. 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.

Obtenu pour vous par
Got for you by
agence europe

ANNEX III
HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(~~2~~3)

In each of the areas listed under points 1-8, the AI systems specifically mentioned under each letter are considered to be h~~H~~igh-risk AI systems pursuant to Article 6(~~2~~3) ~~are the AI systems listed in any of the following areas~~:

1. Biometric**s** ~~**systems** identification and categorisation of natural persons~~:

   (a) ~~AI systems~~ **Remote b~~B~~iometric identification systems** ~~intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons~~ ~~**without their agreement**~~;

2. ~~Management and operation of~~ ~~c~~**C**ritical infrastructure ~~**and protection of environment**~~:

   (a) AI systems intended to be used as safety components in the management and operation of **critical digital infrastructure,** road traffic and the supply of water, gas, heating and electricity**;**

   ~~**(aa) AI systems intended to be used to control or as safety components in the management and operation of critical digital infrastructure;**~~

   (b) ~~**AI systems intended to be used to control emissions and pollution**~~.

3. Education and vocational training:

   (a) AI systems intended to be used **to** ~~for the purpose of~~ determ**ine**~~ining~~ access**, admission** or **to** assign~~ing~~ natural persons to educational and vocational training institutions **or programmes at all levels**;

   (b) AI systems intended to be used ~~for the purpose of~~ ~~**the purpose of**~~ **to** ~~**assessing**~~ ~~assessing students~~ ~~**natural persons** in~~ ~~**with the view to**~~ **evaluate**~~**ing**~~ **learning outcomes, including when those outcomes are used to** ~~**or**~~ **steer**~~**ing**~~ **the learning process of natural persons in educational and vocational training institutions or programmes at all levels** ~~educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational 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 **to place targeted job advertisements,** ~~for advertising vacancies,~~ **to analyse** ~~screening~~ **and** ~~or~~ filter~~ing~~ **job** applications, **and to** ~~evaluating~~ **evaluate** candidates ~~in the course of interviews or tests~~;

   (b) AI intended to be used **to make** ~~for making~~ decisions on promotion and termination of work-related contractual relationships, **to allocate** ~~for~~ task**s** ~~allocation~~ **based on individual behavior or personal traits or characteristics** and **to monitor** ~~for monitoring~~ and evaluat~~ing~~ performance and behavior of persons in such relationships.

5. Access to and enjoyment of **essential** ~~essential~~ private services and **essential** public services and benefits:

   (a) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for **essential** public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such benefits and services;

Obtenu pour vous par
Got for you by
agence europe

(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 put into service by ~~small scale providers~~ **providers that are micro and small-sized enterprises as defined in the Annex of Commission Recommendation 2003/361/EC** for their own use;

(c) AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid**;**~~.~~

(d) ~~**AI systems intended to be used for insurance premium setting, underwritings and claims assessments.**~~

(e) **AI systems intended to be used for risk assessment and pricing in the case of insurance products that include life and health insurance with the exception of AI systems put into service by providers that are micro and small-sized enterprises as defined in the Annex of Commission Recommendation 2003/361/EC for their own use.**

6. Law enforcement:

(a) AI systems intended to be used by law enforcement authorities **or on their behalf** ~~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 **a natural person to become a** potential victim~~s~~ of criminal offences;

(b) AI systems intended to be used by law enforcement authorities **or on their behalf** as polygraphs and similar tools or to detect the emotional state of a natural person;

(c) ~~AI systems intended to be used by law enforcement authorities **or on their behalf** for law enforcement purposes to detect deep fakes as referred to in article 52(3);~~

(d) AI systems intended to be used by law enforcement authorities **or on their behalf** ~~for~~ **to** ~~evaluation~~ **evaluate** ~~of t~~he reliability of evidence in the course of investigation or prosecution of criminal offences;

(e) AI systems intended to be used by law enforcement authorities **or on their behalf to predict** ~~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 **to assess** ~~assessing~~ personality traits and characteristics or past criminal behaviour of natural persons or groups;

(f) AI systems intended to be used by law enforcement authorities **or on their behalf to profile** ~~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;

~~(g) AI systems intended to be used **by law enforcement authorities or on their behalf** 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 competent public authorities **or on their behalf** as polygraphs and similar tools or to detect the emotional state of a natural person;

(b) AI systems intended to be used by competent public authorities **or on their behalf** to assess a risk, including a security risk, a risk of irregular ~~im~~migration, or a health

Obtenu pour vous par
Got for you by
agence europe

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 competent public authorities **or on their behalf** 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 ~~assist~~ **to be used by** competent public authorities **or on their behalf to examine** ~~for the examination of~~ applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status.

8. Administration of justice and democratic processes:

(a) AI systems intended to ~~assist~~ **be used by** a judicial authority **or on their behalf** ~~in~~ **to interpret** ~~**for** researching and~~ ~~interpreting~~ facts ~~and~~ **or** the law ~~and~~ ~~in~~ **to apply** ~~**for** applying~~ the law to a concrete set of facts.

Obtenu pour vous par
Got for you by
agence europe

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 person/s developing the system the date and the version of the system;

   (c) how the AI system interacts or can be used to interact with hardware or software that is not part of the AI system itself, where applicable;

   (d) the versions of relevant software or firmware and any requirement related to version update;

   (e) the description of all forms in which the AI system is placed on the market or put into service **(e.g. software package embedded into hardware, downloadable, API etc.)**;

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

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

   (h) instructions of use for the user and, where applicable installation instructions;

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;

   (i) the design specifications of the system, namely the general logic of the AI system and of the algorithms; 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 description of the expected output of the system;** 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;

   (j) 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;

   (k) where relevant, the data requirements in terms of datasheets describing the training methodologies and techniques and the training data sets used, **including a general description of these data sets**, ~~including~~ information about ~~the~~ **their** 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);

   (l) assessment of the human oversight measures needed in accordance with Article 14, including an assessment of the technical measures needed to facilitate the

Obtenu pour vous par
Got for you by
agence europe

interpretation of the outputs of AI systems by the users, in accordance with Articles 13(3)(d);

(m) 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;

(n) 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).

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 users; specifications on input data, as appropriate;

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

5. A description of ~~any~~ **relevant** change**s made by the provider** 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 and technical 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).

Obtenu pour vous par
Got for you by
agence europe

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;
5. References to any relevant harmonised standards used or any other common specification in relation to which conformity is declared;
6. Where applicable, the name and identification number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued;
7. Place and date of issue of the declaration, name and function of the person who signed it as well as an indication for, and on behalf of whom, that person signed, signature.

Obtenu pour vous par
Got for you by
agence europe

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.

Obtenu pour vous par
Got for you by
agence europe

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;

(o) the list of AI systems covered under the same quality management system;

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

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

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

(s) 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

Obtenu pour vous par
Got for you by
agence europe

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;

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

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

4.3. The technical documentation shall be examined by the notified body. ~~To this purpose,~~ **Where relevant and limited to what is necessary to fulfil their tasks,** the notified body shall be granted full access to the training, **validation,** and testing datasets used ~~by the provider~~, including, **where appropriate and subject to security safeguards,** through application programming interfaces (API) or other ~~appropriate~~ **relevant technical** 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 and upon a reasoned request, the notified body shall also be granted access to the source code of the AI system~~.

Notified bodies shall be granted access to the source code of the AI system upon a reasoned request and only when the following cumulative conditions are fulfilled:

a) Access to source code is necessary to assess the conformity of the high-risk AI system with the requirements set out in Title III, Chapter 2, and

b) testing/auditing procedures and verifications based on the data and documentation provided by the provider have been exhausted or proved insufficient.

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

Obtenu pour vous par
Got for you by
agence europe

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.

Obtenu pour vous par
Got for you by
agence europe

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

~~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.~~

Providers, authorised representatives and users that are public authorities, agencies or bodies shall submit the information referred to in Part I. Providers or, when applicable, authorised representatives shall ensure that the information on their high-risk AI systems referred to in Part II, 1 to 11 is complete, correct and kept up-to-date. Information laid down in II.12 shall be automatically generated by the database.

Part I. Information related to operators (upon operators'registration)

-1. Type of operator (provider, authorised representative or user);

1. Name, address and contact details of the provider;
2. Where submission of information is carried out by another person on behalf of the **operator** ~~provider~~, the name, address and contact details of that person;

Part II. Information related to the high-risk AI system

1. Name, address and contact details of the provider

2. Name, address and contact details of the authorised representative, where applicable;
3. AI system trade name and any additional unambiguous reference allowing identification and traceability of the AI system;
4. Description of the intended purpose of the AI system; ~~**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, this information shall not include the specific context and conditions of use.**~~
5. Status of the AI system (on the market, or in service; no longer placed on the market/in service, recalled);
6. 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;
7. A scanned copy of the certificate referred to in point ~~7~~**6**, when applicable;
8. Member States in which the AI system is or has been placed on the market, put into service or made available in the Union;
9. A copy of the EU declaration of conformity referred to in Article 48;
10. 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.~~
11. URL for additional information (optional).

12. Name, address and contact details of users

Obtenu pour vous par
Got for you by
agence europe

Obtenu pour vous par
Got for you by
agence europe

ANNEX VIIIa

INFORMATION TO BE SUBMITTED UPON THE REGISTRATION OF HIGH-RISK AI SYSTEMS LISTED IN ANNEX III IN RELATION TO TESTING IN REAL WORLD CONDITIONS IN ACCORDANCE WITH ARTICLE 54a

The following information shall be provided and thereafter kept up to date with regard to testing in real world conditions to be registered in accordance with Article 54a:

1. Union-wide unique single identification number of the testing in real world conditions;

2. Name and contact details of the provider or prospective provider and users involved in the testing in real world conditions;

3. A brief description of the AI system, its intended purpose and other information necessary for the identification of the system;

4. A summary of the main characteristics of the plan for testing in real world conditions;

5. Information on the suspension or termination of the testing in real world conditions.

Obtenu pour vous par
Got for you by
agence europe

ANNEX IX
UNION LEGISLATION ON LARGE-SCALE IT SYSTEMS IN THE AREA OF FREEDOM, SECURITY AND JUSTICE

1. Schengen Information System

   (a) Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals (OJ L 312, 7.12.2018, p. 1).

   (v) Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 (OJ L 312, 7.12.2018, p. 14)

   (w) Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56).

2. Visa Information System

   (a) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA - COM(2018) 302 final. To be updated once the Regulation is adopted (April/May 2021) by the co-legislators.

3. Eurodac

   (a) Amended proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment of 'Eurodac' for the comparison of biometric data for the effective application of Regulation (EU) XXX/XXX [Regulation on Asylum and Migration Management] and of Regulation (EU) XXX/XXX [Resettlement Regulation], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulations (EU) 2018/1240 and (EU) 2019/818 – COM(2020) 614 final.

4. Entry/Exit System

   (a) Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327, 9.12.2017, p. 20).

5. European Travel Information and Authorisation System

Obtenu pour vous par
Got for you by
agence europe

(a) Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).

(x) Regulation (EU) 2018/1241 of the European Parliament and of the Council of 12 September 2018 amending Regulation (EU) 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS) (OJ L 236, 19.9.2018, p. 72).

6. European Criminal Records Information System on third-country nationals and stateless persons

(a) Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 (OJ L 135, 22.5.2019, p. 1).

7. Interoperability

(a) Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa (OJ L 135, 22.5.2019, p. 27).

(b) Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration (OJ L 135, 22.5.2019, p. 85).

Obtenu pour vous par
Got for you by
agence europe