Changes compared the previous version are marked in ***blue***

Compromise proposal on General purpose AI systems/value chain

Recital 49

(49) High-risk AI systems should perform consistently throughout their lifecycle and meet an appropriate level of performance, robustness and cybersecurity in accordance with the generally acknowledged state of the art. ***Performance metrics and their expected level should be defined with the primary objective to mitigate risks and negative impact of the AI system. The expected*** level of ***performance*** metrics should be communicated ***in a clear, transparent, easily understandable and intelligible way*** to the deployers. ***The declaration of performance metrics cannot be considered proof of future levels but relevant methods need to be applied to ensure consistant levels during use. While standardisation organisations exist to establish standards, coordination on benchmarking is needed to establish how these standardised requirements and characteristics of AI systems should be measured. The European Artificial Intelligence Office should bring together national and international metrology and benchmarking authorities and provide non-binding guidance to address the technical aspects of how to measure the appropriate levels of performance and robustness.***

Recital 60a (new)

(60a) (new) Foundational models are a recent development, in which AI systems are developed from algorithms designed with the intention to optimize for generality and versatility of output. Those systems can be trained on a broad range of data sources to accomplish a wide range of downstream tasks, including some for which they were not specifically developed and trained. Those systems can be unimodal or multimodal, trained through various methods such as supervised learning or reinforced learning. Foundational models are often the basis for various AI systems with specific intended purpose. These systems hold growing importance to many downstream applications, combined with their complexity and unexpected impact, as well as the downstream operator's lack of control over the AI system's development and consequent power imbalance. Therefore, due to their 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 more specific requirements and obligations under this Regulation while ensuring a high level of protection of fundamental rights, health and safety. AI systems developed for a limited set of applications that cannot be adapted for a wide range of tasks such as components, modules, or simple multi-purpose AI systems should not be considered foundational models for the purposes of this Regulation.

Recital 60b (new)

(60b) (new) Requirements for foundational models should be broadly applicable (e.g. independent of distribution channels, modality, development methods), to address risks specific to such AI systems and complementary to measures for high-risk AI systems, and which can be coherently implemented taking into account industry state-of-the-art practices. These requirements include risk management, extensive analysis and testing of the general model for unforeseen vulnerabilities, including by competent evaluators.

Article 3
Definitions

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

(1a) (new) 'foundational model' means an AI system that is trained on broad data at scale, is designed for generality of output, and can be adapted to a wide range of distinctive tasks;

(1c) (new) 'large training runs' means the production process of a powerful AI models that require computing resources above a very high threshold.

Article 28
Responsibilities along the AI value chain

1. Any distributor, importer, ***deployer*** or other third-party shall be considered a provider ***of a high-risk AI system (AM 2026)*** for the purposes of this Regulation and shall be subject to the obligations of the provider under Article 16, in any of the following circumstances:

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

   (b) they ***make a substantial modification to*** a high-risk AI system ***that has*** already ***been*** placed on the market or ***has already been*** put into service ***and in a way that it remains a high-risk AI system in accordance with Article 6; (AM 133)***

   (ba) they make a substantial modification to an AI system, , which has not been classified as high-risk and has already been placed on the market or put into service in such manner that the AI system becomes a high risk AI system in accordance with Article 6 (AM 132, 134, 2031, 2032)

2. Where the circumstances referred to in paragraph 1, point (***a***) ***to (ba) ~~or~~ ((AM 135)***, occur, the provider that initially placed the AI system on the market or put it into

service shall no longer be considered a provider ***of that specific AI system*** for the purposes of this Regulation. ***This former provider shall, without compromising its own intellectual property rights or trade secrets, provide the new provider with the technical documentation and all other essential relevant and reasonably expected information capabilities of the AI system, technical access or other assistance based on the generally acknowledged state of the art that are required for the fulfilment of the obligations set out in this Regulation. (AM 2033)***

3. The provider of a high risk AI system and the third party that supplies tools, services, components, including foundation models, or processes that are used or integrated in the high risk AI system shall, by written agreement and without compromising intellectual property rights or trade secrets, specify the information, capabilities, technical access, and or other assistance, based on the generally acknowledged state of the art, that the third party must provide in order to enable the provider of the high risk AI system to fully comply with the obligations under this Regulation.

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

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

Article 28(a) (new)

Unfair contractual terms unilaterally imposed on an SME or startup

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

1a. A contractual term is not to be considered unfair where it arises from applicable Union law.

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

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

(a) exclude or limit the liability of the party that unilaterally imposed the term for intentional acts or gross negligence;
(b) exclude the remedies available to the party upon whom the term has been unilaterally imposed in the case of non-performance of contractual obligations or the liability of the party that unilaterally imposed the term in the case of a breach of those obligations;
(c) give the party that unilaterally imposed the term the exclusive right to determine whether the technical documentation, information or data supplied are in conformity with the contract or to interpret any term of the contract.

3a. A contractual term shall be considered to be unilaterally imposed within the meaning of this Article if it has been supplied by one contracting party and the other contracting party has not been able to influence its content despite an attempt to negotiate it. The contracting party that supplied a contractual term bears the burden of proving that that term has not been unilaterally imposed.

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

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

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

Article 28b (new)

Obligations of the provider of a foundational model

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

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

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

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

(b) design and develop the foundational model in order to achieve throughout its lifecycle appropriate levels of performance, predictability, interpretability, corrigibility, safety and cybersecurity assessed through model evaluation with the involvement of independent experts, documented analysis, and extensive testing during conceptualisation, design, and development,

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

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

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

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

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

5. Providers of foundational models shall in addition comply with art. 28.1(ba) and 2, as well as Article 28a. In the case of foundational models provided as a service such as through API access, the cooperation referred to in Article 28.2 shall extend throughout the time during which that service is provided to or used by the provider of the downstream AI system, in order to enable appropriate risk mitigation, unless the provider of the foundational model transfers the training model as well as extensive and appropriate information on the datasets and the development process of the system or restricts the service, such as the API access, in such a way that the downstream provider is able to fully comply with this Regulation without futher support from the original provider of the foundational model.

5a. Providers of foundational models specifically intended to be used to generate, autonomously or on the basis of limited human input, content such as complex text, images, audio, or video ("generative AI"), shall in addition comply with the transparency obligations outlined in Article 52, implement adequate safeguards against the generation of illegal content in line with the generally-acknowledged state of the art, and document and disclose the use of training data protected under copyright law.

6. Following the placing on the market or putting into use of the foundational model, the provider shall undertake "know your business customer" checks throughout the model's lifetime via random samples as well as an appropriate monitoring of public incidents. Those checks should include capturing downstream providers' intended and actual uses. In case the provider of a foundation model identifies a serious incident or a breach of obligations under Union law, it shall notify without undue

delay the national supervisory authority of the Member States, indicating where that serious incident occurred.

In order to carry out checks referred to in paragraph 5, providers of foundational model shall ensure that the downstream provider can only use their foundation model if prior to the use, they have obtained the following information:

(a) the name, address, telephone number and email address of the downstream provider;

(b) a copy of the identification document of the downstream provider or any other electronic identification as defined by Article 3 of Regulation (EU) No 910/2014 of the European Parliament and of the Council (40).

(c) where the downstream provider is registered in a trade register or similar public register, the trade register in which the trader is registered and its registration number or equivalent means of identification in that register;

(e) a self-certification by the downstream provider committing to only use the foundational model in a way that complies with the applicable rules of Union law.

Article 15
Accuracy, robustness and cybersecurity

1a. (new) To address the technical aspects of how to measure the appropriate levels of accuracy and robustness set out in paragraph 1 of this Article, the AI Office shall bring together national and international metrology and benchmarking authorities and provide non-binding guidance on the matter as set out in Article 56, paragraph 2, point (a).

Article 58
Tasks of the Office

(ca) (new) provide interpretive guidance on how the AI Act applies to the ever evolving typology of AI value chains, and what the resulting implications in terms of accountability of all the entities involved will be under the different scenarios based on the generally acknowledged state of the art, including as reflected in relevant harmonized standards;

(cb) provide particular oversight and monitoring and institutionalize regular dialogue with the providers of foundational models about the compliance of foundational models as well

as AI systems that make use of such AI models with Article 28b of this Regulation, and about industry best practices for self-governance. Any such meeting shall be open to national supervisory authorities, notified bodies and market surveillance authorities to attend and contribute

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

Article 58a (new)
Benchmarking

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

ANNEX VIII

Section C - The following information shall be provided and thereafter kept up to date with regard to general purpose AI systems to be registered in accordance with Article 28b (e).

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

9. ***Description of the results of relevant internal and external testing and optimisation of the model***
10. ***Member States in which the foundation model is or has been placed on the market, put into service or made available in the Union;***
11. ***URL for additional information (optional).***