

EU Artificial Intelligence Act: Microsoft trilogue recommendations

Against the backdrop of final negotiations between the European Parliament, EU Council, and European Commission on the AI Act, Microsoft highlights below the issues it considers crucial for co-legislators to consider and prioritize to ensure the final text achieves its stated aims. In particular, the provisions related to foundation models and their associated requirements (section 1 below) are especially important, as the AI Act should strike the right balance between regulating risks associated with (the application of) such models and allocating responsibilities for risk mitigation at the right level within the technology stack.

FOUNDATION MODELS

1.1 Ensure a risk-based approach to regulating foundation models

Art 4a-c: The Council's General Approach would essentially pre-classify all systems without a specific intended purpose ("**General Purpose AI**"; **GPAI**) as high-risk, capturing a huge and growing number of AI systems, many of which present low risk. By requiring all such AI systems to potentially conform to the strict requirements initially reserved only for high-risk systems, the Council **fundamentally deviates from the risk-based approach** that is at the core of the AI Act. This would risk creating a large and disproportionate compliance burden, particularly for many lower risk systems as well as protracted legal uncertainty in view of the implementing act procedure that will specify and adapt the application of high-risk requirements in the light of such systems' characteristics, technical feasibility, specificities of the AI value chain and of market and technological developments.

Art 3(1c), 28b(1): While the Council approach to GPAI appears intended to address foundation models, we welcome the Parliament's more targeted approach which introduces requirements specifically for such models. We would propose **refining the definition of foundation models further** so as not to conflate them with applications, by clarifying that such models are "intended to be" adapted and "integrated into a range of different downstream applications".

Proposed solution

Delete Council's approach relating to General Purpose AI systems in articles 4a, 4b and 4c.

Retain the Parliament's concept of foundation models as introduced in Article 3 (1c), with changes to clarify that such models are "intended to be" adapted and "integrated into a range of different downstream applications".

[Click here to see our specific amendments \(Annex I, section 1.1\)](#)

1.2 Ensure feasible requirements for foundation model providers

Art 28b: Requirements placed on foundation model providers should **take into account relevant existing legislation as well as the technological realities of the AI value chain**; they should be calibrated to model level risks, be practicable and only extend to what foundation model providers can reasonably address during design and development, rather than all potential risks that downstream applications may present. From this perspective, several requirements proposed by the Parliament in Article 28b are either not appropriate for foundation model providers or risk being disproportionate in practice. This is particularly the case for the following requirements:

- **2(a): Acknowledge that risks are most often context and use-case specific.** While model providers should make significant efforts to mitigate known and identified risks during design and development

stage, they will not be able to reasonably foresee many of the specific use-cases and potential associated risks, which can only be done by the deployer of the specific use case. Therefore, in Article 28b(2)(a) “reasonably foreseeable risks” should be replaced with “identified risks”. Moreover, “non-mitigable risks” should be replaced with “known risks”.

- **2(a, c): Reconsider mandatory involvement of independent experts in development and evaluation phase.** Microsoft has committed to arrange access for auditing by independent experts for new and highly capable AI models that we may develop in the future. However, introducing a strict and blanket requirement to involve independent experts in the development phase of all foundation models would be disproportionate. Moreover, such a broad requirement would be unfeasible in practice due to the current lack of expertise on the nascent market for such auditing services and it is unclear who could qualify as an independent expert under such a requirement.
- **2(c): Keep design requirements focused on factors within the control of the model provider.** We caution against requiring providers of foundation models to ensure appropriate levels of predictability and interpretability throughout a foundation model’s lifecycle, as these factors are heavily influenced by decisions taken by application developers and therefore out of the model provider’s control.
- **2(d): Align environmental impact requirements to dedicated existing and emerging legislation.** Microsoft supports the EU’s efforts for greater transparency and reporting as an important part of the Green Deal and we welcome unified and transparent reporting of sustainability performance that will be based on clear, consistent, and targeted standards, developed in collaboration with industry and other key stakeholders, that provide specific data without jeopardizing security or coherence. We would suggest that any transparency and reporting requirements be fully aligned and compatible with existing, well-established reporting frameworks, as well as emerging rules such as data center sustainability indicators being developed in secondary legislation to the Energy Efficiency Directive review, the CSR Directive, the EU Taxonomy Regulation, and the GHG Protocol.
- **2(e): Calibrate requirements for technical documentation.** We support the introduction of a requirement on foundation model providers to draw up technical documentation and instructions to enable downstream providers to comply with their obligations. Rather than classifying this documentation as “extensive”, these should rather be “appropriate” and focus on details of the provider, a description of the data sources used in development, a description of capabilities and limitations, instructions for use and factors affecting use and should safeguard trade secrets and intellectual property rights of providers.
- **2(c, d, f, g), 3: Protect open source by setting proportional requirements for foundation models that are not commercially deployed.** While several obligations the Parliament text imposes on foundation models are close to the principles underpinning the open-source development model, the current one-size-fits-all approach risks creating insurmountable barriers for participants in the open-source AI ecosystem. Instead, the AI Act should recognize and distinctly treat different uses and development modalities. This can be achieved by exempting models that are not placed on the market from some more far-reaching obligations. We propose that foundation models that are not commercially deployed be exempt from requirements listed in paragraphs 2c, 2d, 2f, 2g and 3. This change would align Article 28b with the intent expressed in Recitals 12a-c in the Parliament text for a tailored approach to regulating open-source AI.
- **4(c): Avoid disproportionate and burdensome copyright training data summaries.** The EU Copyright Directive provides for an explicit and mandatory exception for text and data mining (TDM), based on which rightsholders may reserve their rights, or “opt out” from such TDM. This exception was introduced precisely with machine learning in mind, with the aim of fostering the development of data analytics and AI within the EU.¹ Introducing a requirement to document and disclose a summary of the use of copyright protected works used in training of foundation models fundamentally undermines the purpose of the TDM exception, as this burdensome requirement will discourage the use of TDM. It should be sufficient to demonstrate compliance with the opt-out by ensuring that a TDM user has a process to respect the opt-out and by ensuring that the rightsholder has adopted the appropriate means to opt-out their works.

¹ [Copyright Reform: Questions and Answers | Shaping Europe’s digital future \(europa.eu\)](#)

Proposed solution

Article 28b

(2)(a): replace “reasonably foreseeable” with “identified” risks and replace “non-mitigable” with “known” risks.

(2)(a) + (c): remove references to “independent experts”

(2)(c): remove references to predictability and interpretability levels as these factors are heavily influenced by decisions taken by application developers.

(2)(d): redraft to align requirements to existing energy efficiency and sustainability rules, remove “measurement and logging” requirements throughout system’s lifecycle

(2)(e): replace “extensive” with “appropriate” documentation, add IP and trade secrets safeguard

(4)(c): remove requirement to publish a summary of the use of copyright protected training data

Exempt providers of foundation models that are not placed on the market from requirements listed in paragraphs 2c, 2d, 2f, 2g and 3.

[Click here to see our specific amendments \(Annex I, section 1.2\)](#)

1.3 Establish viable transparency obligations for artificially generated content

Art 52(3): We believe there is **benefit in requiring AI-generated image and audiovisual content to be labeled** in important scenarios so that the public “knows the content” it is receiving. Thoughtful measures to deter the misuse of new technology to deceive or defraud the public will benefit the health of democracy and future of civic discourse. Tools are also being developed that allow for digital watermarking of images and audiovisual content so that people know when such content is artificially generated, where this content originated and if it has been adjusted since its creation. The requirement in the Act that companies should use the generally accepted state-of-the-art tools to label content will therefore allow for the use of the latest and most effective tools. Microsoft is at the forefront of multistakeholder initiatives such as the [Coalition for Content Provenance or C2PA](#)², focusing on developing systems to provide context and history for digital media and integrating this in our public facing services, such as Bing Image Creator.

Art 52(3): Focus transparency requirement on image, audio and video content. The Commission and Council approach rightly focus transparency requirements on AI generated image, audio and video content, or “deep fakes”, that can be used to deceive and distort public conversation. The Parliament adds “text” to the scope of the labeling requirement for deep fakes in Article 52(3). The highly dynamic interaction between text-based AI generated content and user modifications makes it challenging to label such content in a meaningful way beyond the direct interaction of the end-user co-creating the content. It is unlikely that the types of tools developed for labeling image and audio-visual content would be effective for text. Therefore, we suggest focusing on the requirement under Article 52(1) to make sure it is clear for someone that they are interacting with an AI system which is more appropriate to ensure transparency relating to the provenance of text-based content, in combination with risk mitigation measures to be taken by online platforms in the context of the Digital Services Act.

Proposed solution

Revise the Parliament’s text in Article 52 paragraph 3 and 3a, to focus labeling requirements on artificially generated audio and visual content.

[Click here to see our specific amendments \(Annex I, section 1.3\)](#)

² Co-founded by companies such as Adobe, the BBC, Intel, Microsoft, Sony, and Truepic, C2PA unifies the efforts of the Adobe-led Content Authenticity Initiative (CAI), which focuses on systems to provide context and history for digital media, and Project Origin, a Microsoft- and BBC-led initiative that tackles disinformation in the digital news ecosystem.

HIGH-RISK AI SYSTEMS

2.1 Ensure a clear and targeted approach to high-risk

Art 6(2): We support Parliament’s balanced approach to consider AI systems listed in Annex III as high-risk, **only if they pose a significant risk of harm** to the health, safety, or fundamental rights of natural persons (Article 6(2)). This ensures a sufficient link between the use cases listed in Annex III and the actual risks associated with specific AI systems placed on the market.

Art 6(2)(a): Parliament’s proposal to **require providers to notify supervisory authorities** where they consider that a system falling within the category listed in Annex III does not pose a significant risk (Article 6(2)(a)) can lead to enforcement challenges in practice due to supervisory authorities’ lack of resources. Furthermore, diverging interpretations of what constitutes significant risk amongst national competent authorities could lead to legal uncertainties, similar to GDPR enforcement experiences. A more reasonable approach could be to simply require that **providers document the assessment which classifies their AI system as low-risk and make it available upon request to competent authorities**.

Art 6(3): The Council proposed criteria in Article 6(3) of an AI system’s output having to **“not likely lead”** to a significant risk and being **“purely accessory”** nature, with the Commission determining the latter interpretation through implementing acts one year after the entry into force. While the aim of narrowing the high-risk classification is welcome, this approach risks leading to significant and protracted legal uncertainty.

Proposed solution

Retain Parliament’s position in Article 6(2), without the additional notification layer involving competent authorities as described in Article 6(2)(a).

[Click here to see our specific amendments \(Annex I, section 2.1\)](#)

2.2 Maintain a balanced approach to AI value chain

Art 28(1)(ba), 28(2): We welcome Parliament’s balanced approach to responsibilities along the AI value chain in Article 28, whereby the entity making the decision to modify a non-high-risk AI system in a way that makes it high-risk, **becomes a provider for the purposes of the regulation** and must meet its related responsibilities.

We also suggest complementing Article 28 with a new recital to **provide examples of information and other assistance** that may be provided by providers of high-risk AI systems to enable downstream operators’ compliance with the provider’s obligations for high-risk AI systems. The final text should also retain Parliament’s proposed recital 60g, which clarifies that **“multi-purpose” AI systems** should not be included in the scope of the AI Act unless they are integrated into or placed on the market as a high-risk system.

Proposed solution

Retain Parliament’s proposals in Article 28 paragraphs 1(ba) and 2, and recital 60g.

Add a new recital 60aa, corresponding to Article 28, to suggest examples of information and other assistance that may be provided by providers of high-risk AI systems to enable downstream operators’ compliance with the provider’s obligations for high-risk AI systems.

[Click here to see our specific amendments \(Annex I, section 2.2\)](#)

2.3 Align high-risk requirements with existing, dedicated regulation

Annex III: The Parliament's addition to consider AI systems intended to be used by **Very Large Online Platforms (VLOPs) in their recommender systems** as constituting high-risk AI systems under Annex III is strongly duplicative of dedicated and well considered provisions laid down in the Digital Services Act, which has only recently entered into application. Moreover, this provision significantly deviates from the AI Act's risk-based approach as it is unclear which specific risks it concerns and how it relates to the type and size of the entity deploying such systems.

Art 12(2)(a), 41(1)(c), Annex IV: Parliament's added requirements relating to **energy consumption and environmental impact of high-risk AI systems** should be based on clear, consistent, and targeted standards, developed in collaboration with industry and other key stakeholders, that provide specific data without jeopardizing security or coherence. Moreover, the level of detail as proposed does not consider the technical feasibility challenges of logging capabilities along the AI value chain, nor does a system's designation as being high-risk have any bearing on its energy consumption compared to low-risk systems. We recommend any transparency and reporting requirements be fully aligned and compatible with existing, well-established reporting frameworks as well as emerging rules, as mentioned under section 1.3.

Proposed solution

Delete the Parliament's addition to Annex III, paragraph 1, point 8 (ab new) and rather rely on implementation and enforcement of relevant provisions under the Digital Services Act.

Redraft the Parliament's addition in Article 12(2a) on record-keeping requirements for high-risk AI systems and the addition to Annex IV on information requirements in paragraph 3b, to align with existing legislation.

[Click here to see our specific amendments \(Annex I, section 2.3\)](#)

DEFINITIONS, SCOPE AND STANDARDS

3.1 Align definition of AI systems to international best practice

Art 3(1), Annex I: Parliament's definition of an AI system more closely **aligns with international best practice such as OECD and NIST frameworks**, an approach more suitable to development of international standards. We also welcome the deletion by Parliament and Council of the list of AI techniques and approaches in Annex I, as these are overly broad and would risk capturing a broad array of software programs already on the market for many years, such as productivity applications (e.g. Word or Excel). While the Council's amendments to the definition of AI systems are a step in the right direction, they still retain overly broad elements such as the reference to logic and knowledge-based approaches, which could still risk capturing predominantly traditional software.

Proposed solution

Retain the Parliament's definition of AI systems in Article 3(1) and retain the Parliament's and Council's approach by deleting Annex I which lists AI techniques and approaches.

[Click here to see our specific amendments \(Annex I, section 3.1\)](#)

3.2 Refine scope to third-country providers and deployers of AI systems

Art 2(1)(c): While Commission and Council have both proposed to limit scope to third-country providers and deployers whereby output produced by AI systems is used in the EU, Parliament’s addition of “intended to be used” further refines the scope and provides more legal certainty, which will be helpful in the international trade context.

Proposed solution

Retain the Parliament’s proposal in Article 2(1)(c).

[Click here to see our specific amendments \(Annex I, section 3.2\)](#)

3.3 Safeguard the primacy of harmonized standards

Art 41: We strongly support the use of **voluntary harmonized standards** to facilitate the conformity assessment process. Relevant harmonized standards by CEN-CENELEC are currently expected to become available in early 2025, ahead of the AI Act’s entry into application. We strongly advocate for CEN-CENELEC to leverage existing standards and monitor standards currently under development within the International Standards Organization (ISO) to ensure consistency. Standards generated from ISO/IEC JTC 1/SC 42 are particularly important.

Art 41(1c): While we welcome the Parliament’s emphasis on the use harmonized standards, its text unfortunately deviates from the harmonized standards approach in Article 41(1c) by mandating the Commission to directly issue common specifications regarding the methodology for reporting and documentation requirement on the consumption of energy and resources of high-risk systems. It is important to ensure that the **Commission will only develop common specifications in exceptional circumstances** where conventional standards may not be appropriate or are proven to be unfeasible. The standards-making process should first be properly utilized and exhausted, before mandating the development of common specifications by the Commission through a less inclusive process.

Proposed solution

Retain the exceptional circumstances outlined by the Parliament in Article 41(1a)(a-c) that would need to be met before the Commission can develop and adopt common specifications.

Revise the Parliament’s text in Article 41(1c) to ensure the Commission would only be able to develop common specifications if the conditions in Article 41(1a)(a-c) are met.

[Click here to see our specific amendments \(Annex I, section 3.3\)](#)

3.4 Protect collaborative development of open-source AI components

Art 2(5e), Art 3, Rec 12a-c: Parliament offers helpful clarity for the developers and distributors of open-source AI components in Recitals 12a-c. These provisions are essential in order to foster contributions from and enable services for the open-source community in Europe. However, Article 2(5e) appears to contradict Recitals 12a-c, introducing ambiguity on whether foundation models can be collaboratively developed and shared on public repositories per Recital 12b, as distinct from providers placing finished foundation models on the market or putting them into service subject to Article 28b. Article 2(5e) should be revised to **clarify that foundation models are subject to the open-source exemption until they are placed on the market or put into service**. This would provide clarity for open-source developers and their service providers while retaining protections for the safe marketing and deployment of foundation models. Additionally, Recitals 12a-c and Article 2(5e) invoke the undefined term “AI component”; defining it will again provide helpful clarity to protect the collaborative open-source development.

[Proposed solution](#)

Retain the Parliament's partial open-source exemption, and modify Article 2(5e) to eliminate contradictions with Recitals 12a-c.

Define "AI components" in Article 3.

[Click here to see our specific amendments \(Annex I, section 3.4\)](#)

ENFORCEMENT

4.1 Ensure resourced and proportionate enforcement

Art 59, 66a: We welcome the Parliament's approach to enforcement, whereby Member States would **designate a single national supervisory authority** (Article 59), as opposed to the Council and the Commission proposals whereby each Member State could designate multiple national competent authorities. We also welcome Parliament's proposal to **partially centralize some enforcement authorities under an AI Office within the Commission** (Article 66a), which would take on especially serious cases of AI risk in addition to providing support services through a secretariat.

Art 59a(2): The Parliament proposes that in cases where multiple national supervisory authorities are involved, the lead NSA will be where the infringement took place (Article 59a(2)). It remains unclear how the lead NSA would be determined in the case of simultaneous cross-border alleged infringements. We suggest that the **supervisory authority of a company's main establishment should be the only competent authority for decision-making**, including imposing fines. A one-stop-shop mechanism is particularly crucial for companies with separate legal entities and different business lines operating in several Member States, as they need legal certainty as to the one 'lead' regulator being their single point of contact. The one-stop-shop also provides clarity to consumers as to the competent regulator and by ensuring a consistent and more efficient application of the AI Act across Europe.

[Proposed solution](#)

Retain the Parliament's positions in Article 59 and Article 66a.

Amend the Parliament's position in Article 59a(2) to reflect the one-stop-shop principle.

[Click here to see our specific amendments \(Annex I, section 4\)](#)

ANNEX I – PROPOSED SOLUTIONS

Section 1.1 – Ensure a risk-based approach to regulating foundation models

EP: Article 3 – Definitions

(1c) ‘foundation model’ means an AI system model that is trained on broad data at scale, is designed for generality of output, and ~~can be intended to be~~ adapted **and integrated into a variety of downstream applications** to **complete** a wide range of distinctive tasks.

Section 1.2 – Ensure feasible requirements for foundation model providers

EP: Article 28b – Obligations of the provider of a foundation model

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

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

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

(2)(c) design and develop the foundation model in order to achieve throughout its lifecycle appropriate levels of performance, ~~predictability, interpretability,~~ corrigibility, safety and cybersecurity assessed through appropriate methods such as model evaluation ~~with the involvement of independent experts,~~ documented analysis, and extensive testing during conceptualisation, design, and development;

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

(2)(e) draw up ~~extensive appropriate~~ technical documentation and intelligible instructions for use in order to enable the downstream providers to comply with their obligations pursuant to Articles 16 and 28.1, **without compromising their own intellectual property rights or trade secrets;**

(2)(f) set procedures for record keeping of relevant documentation and information establish a quality management system to ensure and document compliance with this Article, with the possibility to experiment in fulfilling this requirement,

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

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

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

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

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

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

~~(4)(c) without prejudice to national or Union legislation on copyright, document and make publicly available a sufficiently detailed summary of the use of training data protected under copyright law.~~

~~(5) Requirements listed in paragraphs 2c, 2d, 2f, 2g and 3 shall only apply to providers of foundation models that are placed on the market.~~

Section 1.3 – Establish viable transparency obligations for AI generated content

EP: Article 52 – Transparency obligations for certain AI systems

(3) Users of an AI system that generates or manipulates **text**, audio or visual content, that would falsely appear to be authentic or truthful and which features depictions of people appearing to say or do things they did not say or do, without their consent (‘deep fake’), shall disclose in an appropriate, timely, clear and visible manner that the content has been artificially generated or manipulated, as well as, whenever possible, the name of the natural or legal person that generated or manipulated it. Disclosure shall mean labelling the content in a way that informs that the content is inauthentic and that is clearly visible for the recipient of that content. To label the content, users shall take into account the generally acknowledged state of the art and relevant harmonized standards and specifications.

(3)(a) Paragraph 3 shall not apply where the use of an AI system that generates or manipulates **text**, audio or visual content is authorized by law or if 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. Where the content forms part of an evidently creative, satirical, artistic or fictional cinematographic, video games visuals and analogous work or programme, transparency obligations set out in paragraph 3 are limited to disclosing of the existence of such generated or manipulated content in an appropriate clear and visible manner that does not hamper the display of the work and disclosing the applicable copyrights, where relevant. It shall also not prevent law enforcement authorities from using AI systems intended to detect deep fakes and prevent, investigate and prosecute criminal offences linked with their use.

Section 2.1 – Ensure a clear and targeted approach to high-risk

EP: Article 6 – Classification rules for high-risk AI systems

(2) In addition to the high-risk AI systems referred to in paragraph 1, AI systems falling under one or more of the critical areas and use cases referred to in Annex III shall be considered high-risk if they pose a significant risk of harm to the health, safety or fundamental rights of natural persons. Where an AI system falls under Annex III point 2, it shall be considered high-risk if it poses a significant risk of harm to the environment. The Commission shall, 6 months prior to the entry into force of this Regulation, following consultation with the AI Office and relevant stakeholders, provide guidelines clearly specifying the circumstances where the output of AI systems referred to in Annex III would pose a significant risk of harm to the health, safety or fundamental rights of natural persons or cases in which it would not.

(2a) Where providers falling under one or more of the critical areas and use cases referred to in Annex III consider that their AI system does not pose a significant risk as described in paragraph 2, they shall **document their assessment and keep the documentation at the disposal of competent authorities. submit a reasoned notification to the national supervisory authority that they are not subject to the**

~~requirements of Title III Chapter 2 of this Regulation. Where the AI system is intended to be used in two or more Member States, that notification shall be addressed to the AI Office. Without prejudice to Article 65, the national supervisory authority shall review and reply to the notification, directly or via the AI Office, within three months if they deem the AI system to be misclassified.~~

Section 2.2 – Maintain a balanced approach to AI value chain

Proposed new recital 60aa, corresponding to Article 28 in the Parliament’s text

Information and other assistance to enable downstream operators’ compliance with the provider’s risk management obligations under Article 9 of this Regulation may include: information about the capabilities and limitations of the model, including a description of the functionality it offers; instructions for how the model should be used; a detailed description of any relevant testing that has been done by or on behalf of the supplier of the foundation model with respect to model performance, including a summary of the testing methodology used; information about steps taken by the supplier of the foundation model to identify and mitigate the known and reasonably foreseeable risks of the model that can be reasonably mitigated through the development or supply of the model (as applicable), and any relevant information to assist providers of high-risk AI systems conducting performance testing as required by the AI Act.

Information and other assistance to enable downstream operators’ compliance with the provider’s data governance obligations under Article 10 of this Regulation, may include: an overview of the types of data on which the model was trained; an overview of how the training data was collected and processed, such as annotation, enrichment, and aggregation (as applicable); the formulation of relevant assumptions in relation to the data, notably with respect to the information that the data are supposed to measure and represent; a qualitative assessment of known biases in the data; and a qualitative assessment of known possible gaps or shortcomings, including any relevant assessment of known biases, in the data.

Information and other assistance to enable downstream operators’ compliance with the provider’s technical documentation obligations under to Article 11 of this Regulation, may include: the name of the model supplier, registered trade name or registered trademark, the address at which it can be contacted; and a general description of the model’s runtime parameters.

Information and other assistance to enable downstream operators’ compliance with the provider’s record keeping obligations under Article 12 of this Regulation, may include documentation about the nature and format of the foundation model’s input and output data.

Information and other assistance to enable downstream operators’ compliance with the provider’s transparency and human oversight obligations under Articles 13 and 14 of this Regulation, may include relevant and appropriate information to help providers draft user documentation that allows a trained user to understand the system’s output and provide oversight.

Information and other assistance to enable downstream operators’ compliance with the provider’s accuracy, robustness, and cybersecurity obligations under Article 15 of this Regulation, may include: detailed description of any relevant testing that has been done by or on behalf of the supplier of the foundation model with respect to model performance, including a summary of the testing methodology used; and any relevant information to assist providers of high-risk AI systems with conducting performance testing as required by the AI Act.

Section 2.3 – Align high-risk requirements with existing, dedicated regulation

EP: Annex III: High-risk AI systems referred to in Article 6(2), Paragraph 1, point 8 (ab new):

~~AI systems intended to be used by social media platforms that have been designated as very large online platforms within the meaning of Article 33 of Regulation EU-2022/2065, in their recommender systems to recommend to the recipient of the service user-generated content available on the platform.~~

EP: Article 12 (2a):

High-risk AI systems shall be designed and developed taking into account energy efficiency and sustainability requirements in line with existing legislation ~~with, the logging capabilities enabling the recording of energy consumption, the measurement or calculation of resource use and environmental impact of the high-risk AI system during all phases of the system's lifecycle.~~

EP: Annex IV: Technical Documentation referred to in Article 11(1), point (3b):

Information about the energy consumption of the AI system ~~during the development phase and the expected energy consumption during use taking into account, where applicable,~~ should align with existing and dedicated reporting requirements under relevant Union and national legislation;

Section 3.1 – Align definition of AI systems to international best practice

EP: Article 3 – Definitions

(3)(1) ‘artificial intelligence system’ (AI system) means a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments.

Annex I: Artificial Intelligence Techniques and approaches, referred to in Article 3, point 1

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

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

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

Section 3.2 – Refine scope to 3rd country providers and deployers of AI systems

EP: Article 2: Scope

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

Section 3.3 – Safeguard the primacy of harmonized standards

EP: Article 41: Common specifications

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

(1a)(a) there is no reference to harmonised standards already published in the Official Journal of the European Union related to the essential requirement(s), unless the harmonised standard in question is an existing standard that must be revised; and

(1a)(b) the Commission has requested one or more European standardisation organisations to draft a harmonised standard for the essential requirement(s) set out in Chapter 2; and

(1a)(c) the request referred to in point (b) has not been accepted by any of the European standardisation organisations; or there are undue delays in the establishment of an appropriate harmonised standard; or

the standard provided does not satisfy the requirements of the relevant EU legislation, or does not comply with the request of the Commission.

(1c) The Commission **shall may only** develop common specifications for the methodology to fulfil the reporting and documentation requirement on the consumption of energy and resources during development, training and deployment of the high risk AI system **when the conditions outlined in Article 41 paragraph 1a are fulfilled.**

Section 3.4 – Protect collaborative development of open-source AI components

Article 2: Scope

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

Article 3: Definitions

(3)(1)(f) ‘AI component’ means any software element required to build and operate an AI system, including software code, training data, a model and its weights.

Section 4.1 – Protect collaborative development of open-source AI components

EP: Article 59a – Cooperation mechanism between national supervisory authorities in cases involving two or more Member States

(2) In the event of a case involving two or more national supervisory authorities, the national supervisory authority **of a company’s main establishment of the Member State where the infringement took place** shall be considered the lead supervisory authority.