High-level Recommendations

- Preserve the technology-neutral, risk-based approach of the Commission's proposal regarding foundation models.
- Rebalance the allocation of responsibilities between developers and deployers.
- Align the definition of AI systems with the OECD's definition.
- Narrow down the definition of high-risk AI and allow for flexibility.
- Limit the scope of high-risk AI in Employment to uses which are actually high-risk.
- Ensure that trade secrets and source code are adequately protected.

Detailed Recommendations

Scope **(Art. 2)**	
Recommendation: EP position ***amended***	5d. This Regulation shall not apply to research, testing and development activities regarding an AI system prior to this system being placed on the market or put into service, provided that these activities are conducted respecting fundamental rights and the applicable Union law. 5e. This Regulation shall not apply to AI components provided under free and open-source licenses 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.***~~
Justification	Consistent with the risk-based approach, research activities in the AI field should not be included in the scope of the Act until they are placed on the market and into a high-risk use. The same exemption should apply to open-source AI from the scope of the Act, unless placed on the market directly as part of a high-risk AI system. This exemption should however apply also to open source used for foundation models, to ensure consistency with the Act's technology-neutral approach.

Definition of AI Systems **(Art. 3)**	
Recommendation: EP position	3(1). Artificial intelligence 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.

Justification	The Commission's definition of AI systems as well as its Annex I are extremely broad and cover software and techniques which are not considered to be AI. The European Parliament's definition of AI is closer to the OECD's and other international initiatives.

Definition of High Risk (Art. 6)	
Recommendation: EP position	6(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**. **6(2a). Where providers falling under one or more of the critical areas and use cases referred to in Annex III consider that their AI system does not pose a significant risk as described in paragraph 2, they shall submit a reasoned notification to the National Supervisory Authority that they are not subject to the requirements of Title III Chapter 2 of this Regulation. Where the AI system is intended to be used in two or more Member States, the aforementioned notification shall be addressed to the AI Office. Without prejudice to Article 65, the National Supervisory Authority shall review and reply, directly or via the AI Office, within 3 months if they deem the AI system to be misclassified.**
Justification	A clear yet flexible definition of high-risk AI is very important for future compliance. The European Parliament's proposal fine tunes this definition through the reminder that only uses which pose a significant risk of harm should be covered. It also provides flexibility to providers who do not believe their AI system is high-risk to justify this position to a supervisory authority.

High Risk AI Systems (Annex III)	
Recommendation: Council position	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, to analyse and filter job applications, and to evaluate candidates; **(b) AI intended to be used to make decisions on promotion and termination of work-related contractual relationships, to allocate tasks based on individual behavior or personal traits or characteristics and to monitor and evaluate performance and behavior of persons in such relationships.**
Justification	It is important to differentiate between applications in the area of Employment and Human Resources according to actual risk. The Council provides a much-needed clarification to section 4 by narrowing the scope to uses which are actually high risk.

Requirements for Risk AI Systems (Art.8-15)	
Recommendation: EP and Council positions	
Justification	Requirements for high-risk systems in the original draft include rules which lack legal clarity and flexibility for compliance. As a general rule, compliance with all the requirements should be based on technical feasibility and should encourage stakeholders to meet high levels of quality through best efforts and according to state-of-the-art practices, within the context of the systems’ intended purpose, instead of imposing unrealistic, prescriptive requirements. A more flexible approach that allows for addressing risk according to best practices and the context of intended use will achieve more tailored and effective risk mitigation. Amendments from Council and Parliament generally align with this position.

Allocation of Responsibilities	
Recommendation: EP or Council positions	EP Art. 28.1. **(b a) they make a substantial modification to an AI system, including a general purpose AI system, which has not been classified as high-risk and has already been placed on the**

	market or put into service in such manner that the AI system becomes a high risk AI system in accordance with Article 6. Council Art.23a.1 **(d) they modify 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 which makes the modified system a high-risk AI system;** **(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.**
Justification	Both the Parliament and Council have added that the entity that deploys a non high-risk AI into high-risk setting is responsible for compliance with the AI Act. This makes sense since in many cases it is the deployer that decides the intended purpose of an AI system and is therefore better placed to comply with the requirements for high-risk AI.

GPAI / Foundation Models (1)	
Recommendation: EP position	**Recital 60(g) Pre-trained models developed for a narrower, less general, more limited set of applications that cannot be adapted for a wide range of tasks such as simple multi-purpose AI systems should not be considered foundation models for the purposes of this Regulation, because of their greater interpretability which makes their behaviour less unpredictable.**
Justification	We fully support this exemption since general purpose tools and APIs serve as components of AI systems but are not AI systems per se, and are developed into AI systems by users who also define their intended purpose. It is equally important to differentiate simple multi-purpose AI systems from foundation models, especially public-facing foundation models.

GPAI / Foundation Models (2)	
Recommendation: EP position ***amended***	Article 28b 1. A provider of a foundation model shall, prior to making it available on the market or putting it into service, ensure that it is

	compliant with the requirements set out in this Article, ***to the best of their ability and taking into account the specificities of the AI system. Downstream providers and deployers shall be responsible for ensuring compliance with the requirements set out in this article for their respective continued provision and deployment of such foundation models.*** 2.For the purpose of paragraph 1, the provider of a foundation model shall: (a) demonstrate through appropriate design, testing and analysis that the identification, the reduction and mitigation of ***identified risks*** ~~***reasonably foreseeable risks***~~ to health, safety, fundamental rights, ~~***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; (b) process and incorporate only datasets that are subject to appropriate data governance measures for foundation models, in particular measures to examine the suitability of the data sources and possible biases and appropriate mitigation; c) design and develop the foundation model ~~***in order***~~ ***to the best of their ability*** to aim for appropriate levels of performance, predictability, interpretability, corrigibility, safety and cybersecurity assessed through appropriate methods such as ~~***model evaluation with the involvement of independent experts***~~, documented analysis, and extensive testing during ~~***conceptualisation, design, and***~~ development; (d) design and develop the foundation model, making use of applicable standards to reduce energy use, resource use and waste, as well as to increase energy efficiency, and the overall efficiency of the system. This shall be without prejudice to relevant existing Union and national law and this obligation shall not apply before the standards referred to in Article 40 are published. ~~***They shall be designed with capabilities enabling the measurement and logging of the consumption of energy and resources, and, where technically feasible, other environmental impact the deployment and use of the systems may have over their entire lifecycle***~~;

	(e) draw up extensive technical documentation and intelligible instructions for use in order to enable the downstream providers to comply with their obligations pursuant to Articles 16 and 28.1., ***this requirement does not in any way constitute an obligation to share information or documentation that is business confidential or otherwise constitute a trade secret;*** 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 ***1 year*** ~~***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***~~ ***Deployers*** of foundation models used in AI systems specifically intended to generate ***and disseminate to the public***, with varying levels of autonomy, content such as complex text, images, audio, or video ("generative AI") and ~~***providers***~~ ***deployers*** who specialise a foundation model into a generative AI system ***used to disseminate information to the public***, shall in addition a) comply with the transparency obligations outlined in Article 52 (1), ~~***b) train, and where applicable, design and develop the foundation model in such a way as to ensure adequate safeguards against the generation of content in breach of Union law in line with the generally acknowledged state of the art, and without prejudice to fundamental rights, including the freedom of expression,***~~ ~~***c) without prejudice to national or Union legislation on copyright, document and make publicly available a sufficiently detailed summary of the use of training data protected under copyright law.***~~
	~~***Annex VIII – Information to be submitted upon the registration of High Risk Systems in accordance with Article 51***~~

	~~***Section C - The following information shall be provided and thereafter kept up to date with regard to foundation models to be registered in accordance with Article 28b (e):***~~ ~~***1. Name, address and contact details of the provider;***~~ ~~***2. Where submission of information is carried out by another person on behalf of the provider, the name, address and contact details of that person;***~~ ~~***3. Name, address and contact details of the authorised representative, where applicable;***~~ ~~***4. Trade name and any additional unambiguous reference allowing the identification of the foundation model***~~ ~~***5. Desription of the data sources used in the development of 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 optimization 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).***~~
Justification	We are concerned with both the Parliament's and the Council's proposals to impose requirements on developers of general purpose AI and foundation models regardless of their use. Imposing a risk assessment, mitigation and management requirement for all foundation models would effectively treat foundation models as high-risk applications, regardless of risk. This deviates from the Commission's risk-based approach and makes compliance impossible since developers cannot predict all

	potential applications and thus cannot identify and mitigate every conceivable risk. The Parliament's approach to impose minimum standards could be followed, but needs significant changes that better reflect what developers could actually comply with and what would be most effective at mitigating risk: ○ Developers are only able to deal with identified risks. Deployers decide over the intended purpose of AI systems and foundation models and are therefore better placed to comply with risk mitigation requirements. ○ A requirement to mitigate risks to "democracy, rule of law and the environment" would be difficult to comply with considering that these principles can be interpreted in many ways. ○ Assuming that developers have a full understanding of a model's capabilities and limitations would be inexact. Requirements to provide information should be limited to intended capabilities and limitations. ○ A requirement to assess a model's performance by external experts will be difficult to comply with, considering the lack of such experts on the market. Similarly, it does not make sense to refer to public benchmarks in legislation since they are only just emerging. References to industry best practices might make more sense and is a flexible and future proof approach as such standards evolve and improve over time. ○ A requirement to share "extensive technical documentation" is very broad and could violate trade secret protection. ○ The requirement to register all foundation models in a database would not add anything to the Act's objectives and is further complicated by the fact that deployers make changes to foundation models and it is unclear as to who has the responsibility to register in that case. ○ A 10 year record-retention requirement is unnecessary, particularly when considering that the foundation model

	may be updated frequently or removed from production. ○ Regarding generative systems, the Act should focus on generative systems which disseminate information to the public. Generative systems used in closed enterprise domains do not carry the same risks as consumer-facing systems and any risks that may arise are contained and can be addressed. ○ It would be technically impossible to ensure that generative systems do not generate content in breach of Union law. Best efforts at risk mitigation should be required instead. It is also very difficult to document and make publicly available a summary of the use of training data protected under copyright law. There already are requirements related to data sets and personal data and IP rights. This requirement does not add anything in terms of regulatory protection and is duplicative.

Access to Data in Enforcement (Art. 64)	
Recommendation: EP position ***amended***	Art. 64 (2). Where necessary to assess the conformity of the high-risk AI system with the requirements set out in Title III, Chapter 2, **after all other reasonable ways to verify conformity including paragraph 1 have been exhausted and have proven to be insufficient,** and upon a reasoned request, the **national supervisory authority** shall be granted access to the training and **trained models** of the AI system**, including its relevant model parameters. All information in line with Article 70 obtained shall be treated as confidential information and shall be subject to existing Union law on the protection of intellectual property and trade secrets and shall be deleted upon the completion of the investigation for which the information was requested.** ~~*(79)* ***In cases of simpler software systems falling under this Regulation that are not based on trained models, and where all other ways to verify conformity have been exhausted, the national supervisory authority may exceptionally have access to the source code, upon a reasoned request.***~~

Justification	The European Parliament rightfully deleted references to source code in Art. 64(2) and instead added the possibility for market surveillance authorities to request access to trained models and model parameters. This makes more sense from a technical perspective and would also ensure legal protection for trade secrets. Accessing source code would not only provide very little understanding for possible concerns, it would also set a dangerous precedent limiting IP protection. The useful amendment by the Parliament is nevertheless inconsistent with an addition to Recital 79 which should be removed, as it mentions that *"in cases of simpler software systems falling under this Regulation that are not based on trained models, and where all other ways to verify conformity have been exhausted, the national supervisory authority may exceptionally have access to the source code, upon a reasoned request".*