
Position Paper

EU AI Act Trilogues

July 2023

Executive Summary

We welcome the progress achieved in the EU Artificial Intelligence Act legislative process. This paper provides views on the upcoming trilogue negotiations and recommendations aimed at achieving the development of a fair, competitive and safe Artificial Intelligence in Europe. Our key priorities are that:

- **Definitions:** these should be clear, concise and future proof, e.g. focusing on characteristics rather than techniques or examples.
- **General Purpose AI:** we support a single definition for GPAI, rather than splitting into general purpose AI systems and foundation models. Requirements for GPAI providers should focus on ensuring they provide the necessary information to deployers to comply with this regulation when these models are adapted for high-risk use cases.
- **High-risk AI Systems:** we support a proportionate approach which focuses on risk of harm to the health, safety or fundamental rights of natural persons and does not impose unnecessary administrative requirements on industry. We also welcome the involvement of relevant stakeholders by the Commission on the provision of guidelines specifying the circumstances where the output of AI systems would pose a significant risk of harm to the health, safety or fundamental rights of natural persons. We agree that the database requirements should be limited to public authorities. We also strongly support a requirement to consult with affected industry on changes to the scope of high-risk systems.
- **Data Governance:** we support amendments which clarify and make proportionate the requirements on data sets and training data.
- **Supervision Model for Financial Services:** we support that financial institutions' compliance with this regulation should be supervised by financial authorities and that this should be harmonised across the Union.
- **Codes of Conduct:** We welcome the possibility of being able to rely on voluntary codes for the development of a trustworthy AI across the EU. However, we consider that asking for a voluntary adhesion to codes of conduct for non-high risk AI systems reproducing same strict requirements for high-risk AI systems. This would be excessive - a more proportionate approach is needed.

Introduction

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to engage on the ongoing negotiations for the Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence ("The Proposed Act"). Artificial Intelligence (AI) has the potential to deliver significant benefits for wholesale markets participants across areas such as operational efficiency, client offerings, regulatory compliance, cybersecurity and risk management. However, with AI still in the early stages of development and adoption, it is critical that applicable regulation actively fosters innovation, as well as encouraging good governance and risk management practices. The Proposed Act will therefore have profound implications for the future of AI in EU wholesale markets. We support the overall goal to encourage the adoption of trustworthy AI within the EU

Association for Financial Markets in Europe

London Office: Level 10, 20 Churchill Place, London E14 5HJ, United Kingdom T: +44 (0)20 3828 2700

Brussels Office: Rue de la Loi 82, 1040 Brussels, Belgium T: +32 (0)2 883 5540

Frankfurt Office: Neue Mainzer Straße 75, 60311 Frankfurt am Main T: +49 (0)69 710 456 660

www.afme.eu

economy and to ensure that AI is safe and lawful. However, we continue to caution against any approach that is not future proof or that will inhibit innovation.

This paper sets out our recommendations for the trilogue negotiations between the European Parliament (“EP”) and Council in key areas of the proposed Act. An annex to the paper details our proposed drafting suggestions.

1. Definitions – Article 3

As a general comment on language, we support the Council’s use of the term “*financial institutions*” throughout the Proposed Act, rather than the original “*credit institutions*”, which the EP retains. Not all financial services firms who will be subject to this legislation are “*credit institutions*” as regulated by Directive 2013/36/EU. Therefore, use of the broader term “*financial institutions*” is a more comprehensive term which supports a level playing field approach in the financial sector.

In relation to the definitions in the Proposed Act, we would like to highlight the following:

Artificial Intelligence System – Article 3(1)

We believe that, in order for the definition to be workable and future proof, it should focus on the characteristics of AI (for example, a level of autonomy), rather than individual techniques (for example logic-based approaches). This will ensure that the definition remains relevant as AI continues to advance, while also ensuring that non-AI models are not unintentionally within scope. In addition, the EP proposal is largely aligned with NIST¹, ENISA² and OECD³ and the sharing of fundamental concepts and definitions fosters standards and regulations interoperability.

- *Recommendation:* We support the adoption of the EP definition of “*artificial intelligence*”, with the addition of “content” as a possible output, per the Council drafting.

General Purpose AI System and Foundation Models – EP Article 3(1c and 1d); Council Article 3(1b)

We believe that the EP definitions of “*general purpose AI system*” (GPAI) and “*foundation model*” are not sufficiently differentiated. Indeed, we are concerned that there may not be sufficient clarity within the Proposed Act as a whole on the terminology used. Sometimes the expression “*AI model*” (not defined) is used, rather than “*AI system*”, without clarity on whether a difference is intended. Furthermore, while Stanford University has provided a definition for foundation models⁴, there is no universally agreed definition. Inclusion of a definition at this point therefore may not sufficiently futureproof provisions related to foundation models in the Proposed Act.

As a more general point, we also believe there is a lack of clarity as to the difference between a “model” and a “system”. For example in Article 3, the definition of “large training runs” (“*means the production process of a powerful AI model that require computing resources above a very high threshold*”) talks about an AI model, while the definition of “training data” (“*means data used for training an AI system through fitting its learnable parameters*”) talks about an AI system. It is our understanding that the Proposed Act is designed to target systems, providing for a more outcome-based approach to regulation, rather than regulating distinct models. As such, it is not consistent to have a distinct definition of foundation model, and have separate obligations for these models.

Furthermore, it is not clear whether a GPAI system is a subclass of foundation models, the other way around, or neither of the two. Moreover, it is uncertain whether the rules applicable to the foundation models (such as

¹ <https://csrc.nist.gov/Topics/technologies/artificial-intelligence>

² <https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research>

³ <https://oecd.ai/en/ai-principles>

⁴ <https://fsi.stanford.edu/publication/opportunities-and-risks-foundation-models>

EP Article 28b) apply also to GPAI systems. We believe that using the term “*general purpose AI system*” in opposition to “*AI Systems with an intended purpose*” would prevent gaps in the AI Act scope from arising. We cover this point further under Section 3 below.

We also suggest that it would be better for examples of functions performed by GPAI to be retained in the recitals but not included in the definition. The inclusion of examples in a definition risks creating inadvertent loopholes, given that the list would not be exhaustive, and also may render the definition not future-proof.

- *Recommendation:* We suggest that the definition of “*foundation model*” is not retained and that the more concise EP definition of “*general purpose AI*” is retained, with the addition of the Council’s text that “*general purpose AI system may be used in a plurality of contexts and be integrated in a plurality of other AI systems*”. We also suggest removing the use of the expression “*AI model*” from the rest of the Act.

User/Deployer and Affected Person – Article 3(4) and (EP 8a)

A key concern for our members was the potential for confusion regarding the level at which the “*user*” of an AI model should be identified, e.g. whether a firm or an individual. Therefore, we support the EP’s suggestion to change “*user*” to “*deployer*”, which we feel makes it clearer that, for our members, the “*deployer*” would be the financial services firm, not an individual employee.

- *Recommendation:* We support the EP proposal to change “*user*” to “*deployer*” and its proposal to add a definition of “*affected person*”.

Substantial Modification – Article 3(23)

We are pleased that both the EP and Council have addressed concerns raised that changes foreseen ahead of the deployment of an AI application should not be caught within the definition of “*substantial modification*”.

- *Recommendation:* We believe that the EP proposal for amending the definition of “*substantial modification*” is clearer.

Deep Fake – EP Article 3(44d)

To assist with intelligibility, we support efforts to ensure that all definitions are contained within Article 3, as opposed to elsewhere within the Proposed Act. However, it should be noted that the EP’s definition in Article 3 is limited to content resembling “*persons*”, whereas the definition that the Council retains in Article 52(3) takes a broader approach, referencing “*persons, objects, places or other entities or events*”. We believe that this broader scope would be more effective for the financial sector, for example, where deep fakes could undermine trust in financial institutions.

- *Recommendation:* We support the EP proposal to include a definition of “*deep fake*” in Article 3, subject to the inclusion of the Council’s wording on “*persons, objects, places or other entities or events*”.

2. General Principles – EP Article 4a

While we agree with the content of the principles and the intention to link the Proposed Act back to previous EU work on Trustworthy AI⁵, we have concerns about how these can in practice be incorporated into a Regulation. In particular, it is unclear what method would be used to assess compliance. There is also, as the EP drafting notes, an overlap with the Proposed Act’s requirements for high risk AI systems and foundation models.

- *Recommendation:* We do not support the insertion of EP Article 4a. This would be better left to inclusion within the recitals.

⁵ <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>

3. GPAI and Foundation Models – EP Article 28b; Council Articles 4a, 4b and 4c

Acknowledging the recent public focus on GPAI, we support the intention of the EP and Council to ensure that this type of AI is appropriately covered by the Proposed Act. GPAI providers are the sole holders of technical knowledge and are fully aware of design choices and potential trade-offs. However, we caution against any approach which leaves ambiguity regarding definitions or places unreasonable obligations on GPAI. In particular, the balance of accountability between providers and deployers should be considered.

We have made comments in relation to the definitions under Section 1 above, i.e. we believe that a single definition of GPAI (which is drafted to inherently include foundation models) would give the greatest clarity and would prevent any gaps in AIA scope from arising. We also believe that the EP's definition of GPAI is preferable.

In relation to the requirements on GPAI, we suggest beginning with the EP's approach and applying this to GPAI rather than foundation models. This puts obligations upon the provider which would assist the user/deployer and avoid situations in which the user/deployer does not have the required transparency over the data and design of the GPAI system. We also consider that this approach is more tailored to GPAI, whereas the Council articles refer back to the more general provisions in Article 16.

However, we request that consideration is given to how the requirements set out in EP Article 28b can be tailored to the risk level presented by the individual GPAI system. Applying the requirements to all GPAI systems would be disproportionate, particularly given that the rest of the Regulation differentiates between AI systems on a risk basis. A more proportionate approach would be to reinforce the transparency requirements that the providers of GPAI systems have to meet, so that only when a user/deployer decides to adapt these systems to high-risk use cases would the requirements in Title III Chapter 2 of the AIA apply. Therefore, we suggest that it could be sufficient for EP Article 28b (2) to read that the provider of a general purpose AI system should "*provide information on*" rather than "*demonstrate*" compliance with the subsequent sub-paragraphs. This would allow potential deployers/users to decide if a GPAI system can be adapted to cater for a high-risk use case.

We note that this proportionality would require certain additional modifications to the sub-paragraphs of EP Article 28b (2) and have suggested these in the Annex.

- *Recommendation:* We support the EP's approach as set out in EP Article 28b, (1) applying this to GPAI rather than foundation models and (2) only requiring providers of GPAI to put sufficient information at the disposal of potential deployers/users to decide if a high-risk AI system can be based on the GPAI system.

4. Prohibited Practices (Article 5, Recital 17)

We understand the wider concerns on the use of Social Scoring and the possible creation of unacceptable risks for natural persons' health, safety or their fundamental rights. However we note that its definition and scope are wide (and, particularly for the private sector, less clear) as are the potential interpretations of the wording "*detrimental or unfavourable treatment*" included in Article 5. For instance, in principle, the use of AI for the processing of an individual's financial information to ascertain their eligibility for the provision of financial services could now be considered as "*high risk*" because of the "*serious consequences*" and the potential for "*financial exclusion and discrimination*".

Therefore, we support the clarification provided by the Council in Recital 17 that the prohibition "*should not affect lawful evaluation practices of natural persons done for one or more specific purpose in compliance with the law*". This would prevent the prohibition from unintentionally capturing, for example, the use of AI for segmenting clients for marketing campaigns.

- *Recommendation:* We welcome the Council's amendment to Recital 17 that *"This prohibition should not affect lawful evaluation practices of natural persons done for one or more specific purpose in compliance with the law"*.

5. High Risk AI Systems (Article 6, 7, Annex III)

It is important that the definition of high-risk AI systems focuses on the risk of harm to the health, safety or fundamental rights of natural persons, rather than solely on the task which the AI system is designed to perform. Therefore, while we note the intention of the Council amendment to exclude systems that are *"purely accessory"*, we believe that this would be a less appropriate measure than the EP's focus on risk of harm to the health, safety or fundamental rights. To this end, we largely support the definitional amendments to Article 6 proposed by the EP.

In relation to AI systems which are to be excluded from the high-risk designation, we also do not believe that it is proportionate to require notification as proposed by the EP in Article 6(2a). This would in effect be an approval system, rather than a notification system, given that the AI Office would have three months in which to disagree with the notification. It would also require additional supervisory resource. Instead, we suggest that the obligation should be on firms to make a self-assessment, which could be evidenced to a supervisor upon request.

- *Recommendation:* We support the EP proposed amendments to Article 6 with respect to the focus on risks of harm to the health, safety of fundamental rights of natural persons. Furthermore, we support the EP insertion of Article 6(2), second subparagraph, requiring relevant stakeholders to be consulted by the Commission for the provision of guidelines 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.
- *Recommendation:* We do not support the EP insertion of the notification requirement in Article 6(2a).

In relation to Article 7, we believe that there should be consultation of affected industry when changes to Annex III are proposed. More detail on the process by which this would occur would be very welcome.

- *Recommendation:* We support the EP insertion of Article 7(2a) that relevant groups should be consulted when the Commission assesses use cases for 'high-risk' designation.

On the Annex III use case in relation to biometric assessments, we believe that the intended purpose of the AI system is important and that a broad prohibition is disproportionate.

- *Recommendation:* We support the EP amendment to point 1 on biometrics.

On the Annex III use case in relation to creditworthiness assessments, we support a level playing field for all parts of the financial services industry. It does not make sense that small scale providers should be excluded from this use case. Indeed, the focus is on the effects, not on the entity causing harm to the health, safety, or fundamental rights of natural persons.

- *Recommendation:* We support the EP amendment to point 5b on creditworthiness assessments.

On the Annex III use case in relation to crime analytics, we had previously raised concerns that this could inadvertently capture the use of AI to prevent and detect financial crime, which is a hugely important potential use case for financial services firms.

- *Recommendation:* We support the Council's proposed deletion of point 6g on crime analytics.

6. Data Governance (Article 10)

We welcome the acknowledgement from both the EP and Council that the original text of the Proposed Act contained expectations in relation to data governance that were unnecessarily burdensome and likely to be unattainable. It is critical that requirements on biases, data gaps and errors take into account the nature and scale of the risks posed, as well as the extent to which they can be removed or mitigated.

- *Recommendation:* We support both the EP and Council's addition of qualifying language on biases in Article 10(2)(f). We also support the EP's addition of Article 10(2)(fa), subject to the removal of the requirement to "prevent" biases.
- *Recommendation:* We support the EP amendment to Article 10(2)(g) on the relevance of data gaps.
- *Recommendation:* We support the EP amendment to Article 10(3) on the accuracy of training data sets.

On the processing of special categories of data, we welcome the addition of conditions clarifying when this is permitted, since it gives more certainty to firms. There is always a risk for deployers, including a reputational risk, in requesting access to highly sensitive data with the purpose for avoiding bias.

In addition, we caution against use characterisation of biases as "negative". In the context of fairness, when one speaks of bias, it implies biases that require mitigation. For the sake of clarity, we suggest maintaining a consistent terminology throughout the legislation. If it is necessary to introduce a connotation to the notion of bias, in our opinion "unjust" is much more pertinent with respect to fairness issues. We suggest removing "negative" or, as an alternative, changing it to "unjust", which fits better with the amendment to Article 10(2)(f) above.

- *Recommendation:* We support the EP amendment to Article 10(5), subject to the removal of "negative" in relation to bias detection, or its replacement with "unjust".

On responsibility for compliance, we welcome clarification of how the relationship between the provider and the deployer, noting that this would ideally go beyond data to include other aspects such as design choices. Since the allocation of liability is not always binary, it would be helpful if it could be contractually agreed at a more granular level.

- *Recommendation:* We support the EP insertion of Article 10(6a).

7. Transmission and Provision of Information (Article 13)

We are concerned about the EP's insertion of the requirement to enable providers and users to "reasonably understand the system's functioning" in substitution for the original text of "interpret the system's output". The phrase "system's functioning" may be interpreted in the broad sense of requiring global explanations for the AI system. However, there is a fundamental difference between explaining the output of a system and explaining its global functioning.

At a high level, interpreting a system's output could relate to the rationale based on which the model has provided some specific output, e.g. why a particular product has not been recommended for a particular client. This would be a reasonable requirement. On the other hand, explaining the global functioning of the same system could be how it leverages variables and their relationships to provide outputs for *any* client, which may be very difficult to summarise.

- *Recommendation:* We do not support the EP's amendment to Article 13(1), instead preferring the original Commission wording.

8. Human Oversight (Article 14)

We support the approach taken that human oversight should be "appropriate to the circumstances", although we suggest that "appropriate to the possible risks introduced" would be more precise. To this end, we support

the removal of language such as “*fully understand*” which appeared to conflict with the flexibility afforded by this article. We then have a preference for the EP’s wording “*be aware of and sufficiently understand*”.

- *Recommendation:* We support the EP’s amended wording of Article 14(4)(a) on understanding.

9. Quality Management Systems (Article 17)

In relation to application of this article to financial services firms, we support the broader recognition of the Capital Requirement Directive (2013/36/EU) as retained by the EP. Financial services is a highly regulated sector, therefore recognition of existing requirements is important to avoid duplication of regulations.

- *Recommendation:* We support the original Commission wording on Article 17(3) as retained by the EP.

10. Obligations of Distributors, Importers, Users or Any Other Third-party (Council Article 32a; EP Article 28)

We note that the distributor is liable for all the obligations under this regulation, but welcome provision for “*former providers*” who may hold key information required by the distributor or user/deployer.

- *Recommendation:* We support the EP’s amendment to Article 28.

11. Obligations of Users of High-Risk AI Systems (Article 29)

We consider that the EP’s insertion of a paragraph requiring that firms consult workers representatives before using a high-risk AI system in the workplace is duplicative with the existing obligations under Article 29(6) to complete a data protection impact assessment.

This article would also contradict and/or overlap with national labour regulations, such as the Spanish Royal Decree Law 9/2021, of May 11, amending the revised text of the Workers’ Statute Law (approved by Royal Legislative Decree 2/2015, of October 23). Labour law is not a competence transferred to the Member States, so any rule on this topic should be made via a Directive and not a Regulation.

- *Recommendation:* We consider that the EP’s insertions of Article 29(5a) and (6a) are duplicative of each other and also that (5a) pertains to labour law, which should only be addressed in a Directive, not a Regulation. We suggest that only (6a) is retained.

12. Fundamental Rights Impact Assessment (Parliament Article 29a and Recital 58a)

The new fundamental rights impact assessment (FRIA) that the EP has proposed seems redundant with the requirements set out in this Regulation, which already intend to mitigate those risks. Moreover, it appears to overlap with other requirements set in the regulation for high-risk AI systems in Title III Chapter 2, as well as with those in other pieces of legislation, such as the Privacy Impact Assessment obligations in GDPR.

Therefore, if this Article is to be retained, we suggest that should apply to deployers only for systems which fall under Annex III but which have been evaluated by the provider as *not* posing a significant risk of harm to the health, safety or fundamental rights of natural persons (fitting with the EP’s proposed amendments to Article 6, on which we comment above). In cases where the AI system has fallen under Annex III and evaluated as posing a risk, the deployer should be able to rely on the provider’s existing assessment.

In addition, we believe that this article requires the full commitment of the provider, given that the FRIA requires (specifically when a general purpose AI system/foundation model is adapted to an AI system), extensive knowledge of the training dataset and deep technical knowledge of the system. For example, point (1)(h) “*detailed plan as to how the harms and the negative impact on fundamental rights identified will be mitigated*” may be technically unfeasible for the deployer, particularly as mitigation measures should be implemented at the development phase, as well as subsequently. Indeed, if the deployer has the technical knowledge to perform a retraining of the system and thus substantially modify it, the deployer becomes a provider and has also the necessary competencies to conduct the FRIA.

Finally, we caution against placing requirements on systems not identified as high-risk that are likely to either create bottlenecks, such as additional reporting to supervisory authorities on systems, or be disproportionate, such as notification to stakeholders or public registration.

- *Recommendation:* If the EP's Article 29a is to be retained, we suggest that the start of point 1 is amended to apply only to systems which fall under Annex III but which have been evaluated as not posing a significant risk of harm to the health, safety or fundamental rights of natural persons.
- *Recommendation:* We suggest the deletion of point (1)(d) and (h) and a modification of (j) to make the requirement proportionate.
- *Recommendation:* We suggest deleting the requirement to notify supervisory authorities under paragraph 2.
- *Recommendation:* We suggest deleting paragraphs 4 and 5.
- *Recommendation:* We suggest edits to EP Recital 58a in accordance with all of the above.

13. EU Database for Stand-alone High-risk AI Systems (Articles 51 and 60)

We are concerned about the EP's suggestion that deployers who are not subject to the mandatory registration requirement may voluntarily register their high-risk AI system. Encouraging voluntary uptake of a requirement in a regulation may be likely to introduce a de facto mandatory requirement, which would not be the intention. We suggest that this article should reference only those for whom registration is mandatory.

- *Recommendation:* We do not support the EP's amendments to Article 51(1b) and 60(2a) in relation to voluntary registration by deployers.

14. Reporting of Serious Incidents and of Malfunctioning (Article 62)

AFME welcomed the original Commission proposal, retained by the Council, to require reporting of serious incidents within 15 days (only to providers, not extending this obligation to deployers). This would allow firms to establish the nature of the incident and provide full details to the relevant supervisory authority.

- *Recommendation:* We do not support the EP's amendments to Article 62(1).

15. Supervision Model for Financial Services (Article 63)

It is important that, as an already heavily regulated sector, financial services is subject to an appropriate supervision model. In this respect, we support that financial institutions' compliance with this regulation should be supervised by financial authorities and that this should be harmonised across the Union.

- *Recommendation:* We support the Commission's drafting of Article 63(4), as retained by the EP.

16. Access to Data and Documentation (Article 64)

The ability to grant market surveillance authorities full access to training, validation and testing datasets may be subject to non-disclosure restrictions from regulatory or contractual confidentiality obligations. Furthermore, these requirements may cause cybersecurity concerns.

In addition, to the extent that source code was exposed to a security breach, this would present a material risk from a disclosure of proprietary information perspective, and a vulnerability perspective, should the code be used to potentially manipulate models. We are of the view that source code access is not needed to understand how the AI systems work in practice and could introduce additional cybersecurity risks. It would also be challenging to comply with where the model is sourced from a third party.

Moreover, we understand that testing and training data should be made available during on-site inspections, taking in consideration the volume of data, applicable cybersecurity measures and the availability of non-production environments where AI systems could be tested and analysed.

Finally, the article should not refer to “*application programming interfaces (APIs)*” but should remain technology-neutral rather than suggesting individual techniques.

- *Recommendation:* We support the Council’s deletion of Article 64 paragraphs (1) and (2)

17. Codes of Conduct for Voluntary Application of Specific Requirements

We welcome the possibility of relying on voluntary conduct of conducts for the development of a trustworthy AI across the EU. However, we consider that asking for a voluntary adhesion to codes of conduct for non-high risk AI systems reproducing same strict requirements for high-risk AI systems, would be excessive and that a more proportionate approach is needed.

- *Recommendation:* We suggest amendments to the EP’s drafting of Article 69(1-2) to focus on adherence to the spirit of compliance with the principles underpinning trustworthy AI systems.

18. Entry into Force and Application (Article 85, Recital 88)

While we remain concerned that Article 71 (Penalties) may apply before the rest of the regulation applies, we also note the differing application dates for the regulation itself. A longer implementation period would be preferable to allow firms adequate time to prepare and robust implementation by the industry would also support the EU’s desire to be seen as a leader in this field.

- *Recommendation:* We support the Council’s amendment to Article 85(2)

AFME Contacts

Andrew Harvey
andrew.harvey@afme.eu
+44 (0)20 3828 2694

Fiona Willis
fiona.willis@afme.eu
+44 (0)20 3828 2739

Stefano Mazzocchi
stefano.mazzocchi@afme.eu
+32 479 027 989

Annex – Proposed Wording

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
Recital 17	AI systems providing social scoring of natural persons for general purpose by public authorities or 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	AI systems providing social scoring of natural persons for general purpose may lead to discriminatory outcomes and the exclusion of certain groups. They violate the right to dignity and non-discrimination and the values of equality and justice. Such AI systems evaluate or classify natural persons or groups based on multiple data points and time occurrences related to their social behaviour in multiple contexts or known, inferred or predicted personal or personality characteristics. The social score obtained from such AI systems may lead to the detrimental or unfavourable treatment of natural persons or whole groups thereof in social contexts, which are unrelated to the context in which the data was originally generated or collected or to a detrimental treatment that is disproportionate or unjustified to the gravity of their social behaviour. Such AI systems should be therefore prohibited.	AI systems providing social scoring of natural persons by public authorities or by private actors 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 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. AI systems entailing such unacceptable scoring practices should be therefore prohibited. <i>This prohibition should not affect lawful evaluation practices of natural persons done for one or more</i>	We support the Council's amendment to Recital 17.

Association for Financial Markets in Europe

London Office: Level 10, 20 Churchill Place, London E14 5HJ, United Kingdom T: +44 (0)20 3828 2700

Brussels Office: Rue de la Loi 82, 1040 Brussels, Belgium T: +32 (0)2 883 5540

Frankfurt Office: Neue Mainzer Straße 75, 60311 Frankfurt am Main T: + 49 (0)69 710 456 660

www.afme.eu

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
	collected or to a detrimental treatment that is disproportionate or unjustified to the gravity of their social behaviour. Such AI systems should be therefore prohibited.		<i>specific purpose in compliance with the law.</i>	
EP Recital 58a		<i>Whilst risks related to AI systems can result from the way such systems are designed, risks can as well stem from how such AI systems are used. Deployers of high-risk AI system therefore play a critical role in ensuring that fundamental rights are protected, complementing the obligations of the provider when developing the AI system. Deployers are best placed to understand how the high-risk AI system will be used concretely and can therefore identify potential significant risks that were not foreseen in the development phase, due to a more precise knowledge of the context of use, the people or groups of people likely to be affected, including marginalised and vulnerable groups. Deployers should identify appropriate governance structures in that specific context of use, such as arrangements for human oversight, complaint-handling procedures and redress procedures, because choices in the governance structures can be instrumental in mitigating risks to fundamental rights in concrete use-cases. In order to efficiently ensure that fundamental rights are protected, the deployer of high-risk AI systems should therefore carry out a fundamental rights impact assessment prior to putting it into use. The impact assessment should be accompanied by a detailed plan describing the measures or</i>		<p>We suggest the following edits in lien with our comments on EP Article 29a:</p> <p><i>Whilst risks related to AI systems can result from the way such systems are designed, risks can as well stem from how such AI systems are used. Deployers of <u>high-risk AI systems that may be used in high-risk areas</u> therefore play a critical role in ensuring that fundamental rights are protected, complementing the obligations of the provider when developing the AI system. Deployers are best placed to understand how the high-risk AI system will be used concretely and can therefore identify potential significant risks that were not foreseen in the development phase, due to a more precise knowledge of the context</i></p>

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
		<p><i>tools that will help mitigating the risks to fundamental rights identified at the latest from the time of putting it into use. If such plan cannot be identified, the deployer should refrain from putting the system into use. When performing this impact assessment, the deployer should notify the national supervisory authority and, to the best extent possible relevant stakeholders as well as representatives of groups of persons likely to be affected by the AI system in order to collect relevant information which is deemed necessary to perform the impact assessment and are encouraged to make the summary of their fundamental rights impact assessment publicly available on their online website. This obligations should not apply to SMEs which, given the lack of resources, might find it difficult to perform such consultation. Nevertheless, they should also strive to involve such representatives when carrying out their fundamental rights impact assessment. In addition, given the potential impact and the need for democratic oversight and scrutiny, deployers of high-risk AI systems that are public authorities or Union institutions, bodies, offices and agencies, as well deployers who are undertakings designated as a gatekeeper under Regulation (EU) 2022/1925 should be required to register the use of any high-risk AI system in a public database. Other deployers may voluntarily register.</i></p>		<p><i>of use, the people or groups of people likely to be affected, including marginalised and vulnerable groups. <u>In the case of AI systems that may be used in high risk areas, in relation to which the provider has not identified a significant risk to the health, safety and fundamental rights.</u> Deployers should identify appropriate governance structures in that specific context of use, such as arrangements for human oversight, complaint-handling procedures and redress procedures, because choices in the governance structures can be instrumental in mitigating risks to fundamental rights in concrete use-cases. <u>In these specific cases, in order to efficiently ensure that fundamental rights are protected, the deployer of high-risk AI systems</u> should therefore carry out a fundamental rights impact assessment prior to putting it into use. The impact assessment should be accompanied by a</i></p>

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
				<p>detailed plan describing the measures or tools that will help mitigating the risks to fundamental rights identified at the latest from the time of putting it into use. If such plan cannot be identified, the deployer When assessing the systems' impact in the specific context of use, if the deployer identifies a significant risk of harm to the fundamental rights of natural persons, it should refrain from putting the system into use <u>and inform the provider, distributor or authorized representative</u>. When performing this impact assessment, the deployer should notify the national supervisory authority and, to the best extent possible relevant stakeholders as well as representatives of groups of persons likely to be affected by the AI system in order to collect relevant information which is deemed necessary to perform the impact assessment and are encouraged to make the summary of their</p>

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
				<p><u>fundamental rights impact assessment publicly available on their online website. This obligations should not apply to SMEs which, given the lack of resources, might find it difficult to perform such consultation.</u> Nevertheless, they should also strive to involve such representatives when carrying out their fundamental rights impact assessment. <u>In addition, given the potential impact and the need for democratic oversight and scrutiny, deployers of high-risk AI systems that are public authorities or Union institutions, bodies, offices and agencies, as well as deployers who are undertakings designated as a gatekeeper under Regulation (EU) 2022/1925 should be required to register the use of any high-risk AI system in a public database. Other deployers may voluntarily register.</u></p>
3(1)	'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and	'artificial intelligence system' (AI system) means <i>a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or</i>	'artificial intelligence system' (AI system) means <i>a system that is designed to operate with elements of autonomy and that, based on machine and/or human-</i>	AFME supports the EP definition, subject to one amendment from the Council drafting:

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
	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;	<i>implicit objectives, generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments.</i>	<i>provided data and inputs, infers how to achieve a given set of 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;</i>	‘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 <u>content</u>, predictions, recommendations, or decisions that influence physical or virtual environments.
EP: 3(1c-d) Council: 3(1b)		<i>(1c) ‘foundation model’ means an AI model that is trained on broad data at scale, is designed for generality of output, and can be adapted to a wide range of distinctive tasks; (1d) ‘general purpose AI system’ means an AI system that can be used in and adapted to a wide range of applications for which it was not intentionally and specifically designed;</i>	<i>‘general purpose AI system’ means an AI system that – irrespective of how 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;</i>	AFME supports the EP definition, with the addition of the Council’s drafting on plurality: <i>‘general purpose AI system’ means an AI system that can be used in and adapted to a wide range of applications for which it was not intentionally and specifically designed; a general purpose AI system may be used in a plurality of contexts and be integrated in a plurality of other AI systems;</i>
3(4)	‘user’ means any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is	‘ deployer ’ means any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity;	‘user’ means any natural or legal person, including a public authority, agency or other body, under whose authority the system is used;	AFME supports the EP definition.

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
	used in the course of a personal non-professional activity;			
EP 3(8a)		<i>‘affected person’ means any natural person or group of persons who are subject to or otherwise affected by an AI system;</i>		AFME supports the EP definition.
3(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;	‘substantial modification’ means a modification or a series of modifications of the AI system after its placing on the market or putting into service which is not foreseen or planned in the initial risk assessment by the provider and as a result of which the compliance of the AI system with the requirements set out in Title III, Chapter 2 of this Regulation is affected or results in a modification to the intended purpose for which the AI system has been assessed	‘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 a modification to the intended purpose for which the AI system has been assessed. <i>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.</i>	AFME supports the EP definition.
EP 3(44d)		<i>‘deep fake’ means manipulated or synthetic audio, image or video content that would falsely appear to be authentic or truthful, and which features depictions of persons appearing to say or do things they did not say or do, produced using AI techniques, including machine learning and deep learning;</i>		AFME supports the EP definition, subject to the inclusion of the Council’s language in Article 52(3): <i>‘deep fake’ means manipulated or synthetic audio, image or video content that would falsely appear to be authentic or truthful, and which features depictions of persons, objects, places</i>

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
				<i><u>or other entities or events appearing to say or do things they did not say or do, produced using AI techniques, including machine learning and deep learning;</u></i>
EP 4		Article 4a General principles applicable to all AI systems		AFME does not support the EP's proposed article.
Council 4a-c EP 28b		Article 28b Obligations of the provider of a foundation model <i>1. A provider of a foundation model shall, prior to making it available on the market or putting it into service, ensure that it is compliant with the requirements set out in this Article, regardless of whether it is provided as a standalone model or embedded in an AI system or a product, or provided under free and open source licences, as a service, as well as other distribution channels.</i> <i>2. For the purpose of paragraph 1, the provider of a foundation model shall: (a) demonstrate through appropriate design, testing and analysis that the identification, the reduction and mitigation of reasonably foreseeable risks to health, safety, fundamental rights, the environment and democracy and the rule of law prior and throughout development with appropriate methods such as with the involvement of independent experts, as well as the documentation of remaining non-mitigable risks after development</i>	Article 4a Compliance of general purpose AI systems with this Regulation <i>1. Without prejudice to Articles 5, 52, 53 and 69 of this Regulation, general purpose AI systems shall only comply with the requirements and obligations set out in Article 4b.</i> <i>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.</i> Article 4b Requirements for general purpose AI systems and obligations for providers of such systems <i>1. General purpose AI systems which may be used as high risk AI systems or as components of 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</i>	AFME supports the EP's approach, subject to <ul style="list-style-type: none"> first, it applying to general purpose AI systems rather than foundation models, second, only requiring providers of GPAI to put sufficient information at the disposal of potential deployers/users to decide if a high-risk AI system can be based on the GPAI system, and third, removal of the requirement for developers to register all GPAI systems in the EU database: <u>2. For the purpose of paragraph 1, the provider of a foundation model general purpose AI system shall provide information on its approach to:</u>

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
		<p><i>(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</i></p> <p><i>(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;</i></p> <p><i>(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, without prejudice to relevant existing Union and national law. This obligation shall not apply before the standards referred to in Article 40 are published. Foundation models 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;</i></p> <p><i>(e) draw up extensive technical documentation and intelligible instructions for use, in order to enable the downstream providers to comply with</i></p>	<p><i>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. When fulfilling those requirements, the generally acknowledged state of the art shall be taken into account.</i></p> <p><i>2. Providers of general purpose AI systems referred to in paragraph 1 shall comply, as from the date of application of the implementing acts referred to in paragraph 1, with the obligations set out in Articles 16aa, 16e, 16f, 16g, 16i, 16j, 25, 48 and 61.</i></p> <p><i>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.</i></p> <p><i>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.</i></p>	<p><i>(a) demonstrate through appropriate design, testing and analysis the identification, the reduction and mitigation of reasonably foreseeable risks to health, safety, fundamental rights, the environment and democracy and the rule of law prior and throughout development with appropriate methods such as with the involvement of independent experts, as well as the documentation of remaining non-mitigable risks after development</i></p> <p><i>(b) process and incorporate only datasets that are subject to appropriate data governance measures adopted for foundation models, in particular measures to examine the suitability of the data sources and possible biases and appropriate mitigation</i></p> <p><i>(c) design and develop the foundation model in order to achieve throughout its lifecycle, appropriate levels of performance, predictability, interpretability, corrigibility, safety and</i></p>

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
		<p><i>their obligations pursuant to Articles 16 and 28(1);.</i></p> <p><i>(f) establish a quality management system to ensure and document compliance with this Article, with the possibility to experiment in fulfilling this requirement,</i></p> <p><i>(g) register that foundation model in the EU database referred to in Article 60, in accordance with the instructions outlined in Annex VIII point C.</i></p> <p><i>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 in particular in benchmarking guidance and capabilities referred to in Article 58a;</i></p> <p><i>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 2(e) at the disposal of the national competent authorities.</i></p> <p><i>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</i></p> <p><i>a) comply with the transparency obligations outlined in Article 52 (1),</i></p>	<p><i>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).</i></p> <p><i>6. In complying with the requirements and obligations referred to in paragraphs 1, 2 and 3:</i></p> <p><i>- 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;</i></p> <p><i>- 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.</i></p> <p><i>Article 4c Exceptions to Article 4b</i></p>	<p><i>cybersecurity assessed through appropriate methods such as model evaluation with the involvement of independent experts, documented analysis, and <u>extensive appropriate testing during conceptualisation, design, and development;</u></i></p> <p><i>(d) <u>design and develop the foundation model,</u> 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, without prejudice to relevant existing Union and national law. This obligation shall not apply before the standards referred to in Article 40 are published. <u>Foundation models General purpose AI systems</u> 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;</i></p>

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
		<p><i>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,</i></p> <p><i>c) without prejudice to Union or 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.</i></p>	<p><i>1. Article 4b shall not apply when the provider has explicitly excluded all high-risk uses in the instructions of use or information accompanying the general purpose AI system.</i></p> <p><i>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.</i></p> <p><i>3. When the provider detects or is informed about 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.</i></p>	<p><i>(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);</i></p> <p><i>(f) <u>establishing a quality management system to ensure and document compliance with this Article, with the possibility to experiment in fulfilling this requirement,</u></i></p> <p><i>(g) register that foundation model in the EU database referred to in Article 60, in accordance with the instructions outlined in Annex VIII point C.</i></p> <p><i>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 in particular in benchmarking guidance and capabilities referred to in Article 58a;</i></p>

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
6	<p>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:</p> <p>(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;</p> <p>(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.</p> <p>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.</p>	<p>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:</p> <p>(a) the AI system is intended to be used as a safety component of a product or <i>the AI system</i> is itself a product, covered by the Union harmonisation legislation listed in Annex II,</p> <p>(b) the product whose safety component <i>pursuant to point (a)</i> is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment <i>related to risks for health and safety</i>, 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.</p> <p>2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems <i>falling under one or more of the critical areas and use cases</i> referred to in Annex III shall be considered high-risk <i>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.</i></p> <p><i>The Commission shall, six 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</i></p>	<p>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.</p> <p><i>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.</i></p> <p><i>3. AI systems referred to in Annex III shall be considered high-risk unless the output of the system is purely accessory in respect of the relevant action or decision to be taken and is not therefore likely to 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 the circumstances where the output of AI</i></p>	<p>AFME largely supports the drafting of the EP, subject to the following points:</p> <ul style="list-style-type: none"> • We do not support the inclusion of EP Article 6(2a) or the associated reference to the process in Article 6(2b) or (2c) • We support the inclusion in Council Article 6(3) to an exclusion where “the output of the system is purely accessory in respect of the relevant action or decision to be taken and is not therefore likely to lead to a significant risk to the health, safety or fundamental rights”

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
		<p><i>health, safety or fundamental rights of natural persons or cases in which it would not.</i></p> <p><i>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.</i></p> <p><i>2b. Providers that misclassify their AI system as not subject to the requirements of Title III Chapter 2 of this Regulation and place it on the market before the deadline for objection by National Supervisory Authorities shall be responsible and be subject to fines pursuant to Article 71.</i></p> <p><i>2c. National supervisory authorities shall submit a yearly report to the AI Office detailing the number of notifications received, the related high-risk areas at stake and the decisions taken concerning received notifications</i></p>	<p><i>systems referred to in Annex III would be purely accessory in respect of the relevant action or decision to be taken. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74, paragraph 2.</i></p>	
EP 7(2a)		<p><i>When assessing an AI system for the purposes of paragraphs 1 or 1a the Commission shall consult the AI Office</i></p>		AFME supports the EP's proposed insertion.

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
		<i>and, where relevant, representatives of groups on which an AI system has an impact, industry, independent experts, social partners, and civil society organisations. The Commission shall also organise public consultations in this regard and shall make the results of those consultations and of the final assessment publicly available.</i>		
10(2)(f) and EP (10)(2)(fa)	(f) examination in view of possible biases;	<p>(f) examination in view of possible biases <i>that are likely to affect the health and safety of persons, negatively impact fundamental rights or lead to discrimination prohibited under Union law, especially where data outputs influence inputs for future operations ('feedback loops') and appropriate measures to detect, prevent and mitigate possible biases;</i></p> <p><i>(fa) appropriate measures to detect, prevent and mitigate possible biases;</i></p>	(f) examination in view of possible biases <i>that are likely to affect health and safety of natural persons or lead to discrimination prohibited by Union law</i>	<p>AFME supports the Council's amendment to Article 10(2)(f) and partially supports the EP's amendment to Article 10(2)(fa):</p> <p>(f) examination in view of possible biases <i>that are likely to affect health and safety of natural persons or lead to discrimination prohibited by Union law</i></p> <p><i>(fa) appropriate measures to detect, prevent and mitigate possible biases;</i></p>
10(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) 2016/679,	To the extent that it is strictly necessary for the purposes of ensuring <i>negative</i> bias detection and correction in relation to the high-risk AI systems, the providers of such systems may <i>exceptionally</i> 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	[no change]	<p>AFME supports the EP's amendment, subject to one of the following changes:</p> <p>To the extent that it is strictly necessary for the purposes of ensuring <i>negative</i> bias detection and correction...</p> <p>OR</p>

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
	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.	<p>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. <i>In particular, all the following conditions shall apply in order for this processing to occur:</i></p> <p><i>(a) the bias detection and correction cannot be effectively fulfilled by processing synthetic or anonymised data;</i></p> <p><i>(b) the data are pseudonymised;</i></p> <p><i>(c) the provider takes appropriate technical and organisational measures to ensure that the data processed for the purpose of this paragraph are secured, protected, subject to suitable safeguards and only authorised persons have access to those data with appropriate confidentiality obligations;</i></p> <p><i>(d) the data processed for the purpose of this paragraph are not to be transmitted, transferred or otherwise accessed by other parties;</i></p> <p><i>(e) the data processed for the purpose of this paragraph are protected by means of appropriate technical and organisational measures and deleted once the bias has been corrected or the personal data has reached the end of its retention period;</i></p> <p><i>(f) effective and appropriate measures are in place to ensure availability, security and resilience of processing systems and services against technical or physical incidents;</i></p> <p><i>(g) effective and appropriate measures are in place to ensure physical security of locations where the data are stored and processed, internal IT and IT security governance and management, certification of processes and products;</i></p>		To the extent that it is strictly necessary for the purposes of ensuring <u>negative unjust</u> bias detection and correction...

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
		<i>Providers having recourse to this provision shall draw up documentation explaining why the processing of special categories of personal data was necessary to detect and correct biases.</i>		
EP 10(6a)		<i>Where the provider cannot comply with the obligations laid down in this Article because it does not have access to the data and the data is held exclusively by the deployer, the deployer may, on the basis of a contract, be made responsible for any infringement of this Article.</i>		AFME supports the EP addition.
13(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.	High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable providers and users to reasonably understand the system's functioning . Appropriate transparency shall be ensured in accordance with the intended purpose of the AI system , with a view to achieving compliance with the relevant obligations of the provider and user set out in Chapter 3 of this Title. Transparency shall thereby mean that, at the time the high-risk AI system is placed on the market, all technical means available in accordance with the generally acknowledged state of art are used to ensure that the AI system's output is interpretable by the provider and the user. The user shall be enabled to understand and use the AI system appropriately by generally knowing how the AI system works and what data it processes, allowing the user to explain the decisions taken by the AI system to the affected person pursuant to Article 68(c).	High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent 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.	AFME does not support the EP amendment, instead supporting the original Commission proposal.
14(4)(a)	The measures referred to in paragraph 3 shall enable the individuals to whom human	For the purpose of implementing paragraphs 1 to 3, the high-risk AI	For the purpose of implementing paragraphs 1 to 3, the high-risk AI system shall be provided to the user in	AFME supports the EP's amendment.

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
	oversight is assigned to do the following, as appropriate to the circumstances: (a) fully 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;	<i>system</i> shall <i>be provided to the user in such a way that natural persons</i> to whom human oversight is assigned <i>are enabled</i> , as appropriate <i>and proportionate</i> to the circumstances: (a) <i>be aware of and sufficiently</i> understand the <i>relevant</i> 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;	<i>such a way that natural persons to whom human oversight is assigned are enabled, as appropriate and proportionate to the circumstances: (a) to understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation;</i>	
17(3)	For providers that are credit institutions regulated by Directive 2013/36/ EU, the obligation to put a quality management system in place shall be deemed to be fulfilled by complying with the rules on internal governance arrangements, processes and mechanisms pursuant to Article 74 of that Directive. In that context, any harmonised standards referred to in Article 40 of this Regulation shall be taken into account.	[no change]	For providers that are <i>financial institutions subject to requirements regarding their internal governance, arrangements or processes under Union financial services legislation, the obligation to put in place a quality management system 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 pursuant to the relevant Union financial services legislation.</i> In that context, any harmonised standards referred to in Article 40 of this Regulation shall be taken into account.	AFME supports the Commission's drafting, as retained by the EP.
EP 28 Council 23a	<i>Article 28 Obligations of distributors, importers, users or any other third-party</i> 1. Any distributor, importer, user or other third-party shall be considered a provider for the purposes of this Regulation and shall be subject to the	<i>Article 28 Responsibilities along the AI value chain of providers, distributors, importers, deployers or other third party</i> 1. Any distributor, importer, <i>deployer</i> or other third-party shall be considered a provider <i>of a high-risk AI system</i> for the purposes of this Regulation and shall be subject to the obligations of the provider	<i>Article 23a Conditions for other persons to be subject to the obligations of a provider</i> 1. Any <i>natural or legal person</i> shall be considered a provider <i>of a new high-risk AI system</i> for the purposes of this Regulation and shall be subject to the	AFME supports the EP's amendments

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
	<p>obligations of the provider under Article 16, in any of the following circumstances:</p> <p>(a) they place on the market or put into service a high-risk AI system under their name or trademark;</p> <p>(b) they modify the intended purpose of a high-risk AI system already placed on the market or put into service;</p> <p>(c) they make a substantial modification to the high-risk AI system.</p> <p>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.</p>	<p>under Article 16, in any of the following circumstances:</p> <p>(a) they <i>put their name or trademark on a high-risk AI system already placed</i> on the market or put into service</p> <p>(b) they <i>make a substantial modification to</i> a high-risk AI system <i>that has already been</i> placed on the market or <i>has already been</i> put into service <i>and in a way that it remains a high-risk AI system in accordance with Article 6;</i></p> <p><i>(ba) they make a substantial modification to an AI system, including a general purpose AI system, which has not been classified as high-risk and has already been placed on the market or put into service in such manner that the AI system becomes a high risk AI system in accordance with Article 6</i></p> <p>2. Where the circumstances referred to in paragraph 1, point (a) to (ba) occur, the provider that initially placed the AI system on the market or put it into service shall no longer be considered a provider <i>of that specific AI system</i> for the purposes of this Regulation. <i>This former provider shall provide the new provider with the technical documentation and all other relevant and reasonably expected information capabilities of the AI system, technical access or other assistance based on the generally acknowledged state of the art that are required for the fulfilment of the obligations set out in this Regulation.</i></p> <p><i>Paragraph 2 shall also apply to providers of foundation models as defined in Article 3 when the foundation model is directly integrated in an high-risk AI system.</i></p>	<p>obligations of the provider under Article 16, in any of the following circumstances:</p> <p>(a) they <i>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;</i></p> <p><i>(b) [deleted]</i></p> <p>(c) they make a substantial modification to <i>a high-risk AI system already placed on the market or put into service;</i></p> <p><i>(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;</i></p> <p><i>(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.</i></p> <p>2. Where the circumstances referred to in paragraph 1, point (a) 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.</p> <p><i>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></p> <p><i>(i) the high-risk AI system is placed on the market together with the product</i></p>	

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
		<p><i>2a. The provider of a high risk AI system and the third party that supplies tools, services, components or processes that are used or integrated in the high risk AI system shall, by written agreement specify the information, capabilities, technical access, and or other assistance, based on the generally acknowledged state of the art, that the third party must provide in order to enable the provider of the high risk AI system to fully comply with the obligations under this Regulation.</i></p> <p><i>The Commission shall develop and recommend non-binding model contractual terms between providers of high-risk AI systems and third parties that supply tools, services, components or processes that are used or integrated in high-risk AI systems in order to assist both parties in drafting and negotiating contracts with balanced contractual rights and obligations, consistent with each party's level of control. When developing non-binding model contractual terms, the Commission shall take into account possible contractual requirements applicable in specific sectors or business cases.</i></p> <p><i>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.</i></p> <p><i>2b. For the purposes of this Article, trade secrets shall be preserved and shall only be disclosed provided that all specific necessary measures pursuant to Directive (EU) 2016/943 are taken in advance to preserve their confidentiality, in particular with respect to third parties. Where necessary, appropriate technical</i></p>	<p><i>under the name or trademark of the product manufacturer;</i></p> <p><i>(ii) the high-risk AI system is put into service under the name or trademark of the product manufacturer after the product has been placed on the market.</i></p>	

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
		<i>and organizational arrangements can be agreed to protect intellectual property rights or trade secrets.</i>		
EP 28b		<i>Obligations of the provider of a foundation model</i>		See above re Council Article 4a-c
EP 29(5a) and (6a)		<p><i>(5a) Prior to putting into service or use a high-risk AI system at the workplace, deployers shall consult workers representatives with a view to reaching an agreement and inform the affected employees that they will be subject to the system.</i></p> <p><i>...(6a) Without prejudice to Article 52, deployers of high-risk AI systems referred to in Annex III, which make decisions or assist in making decisions related to natural persons, shall inform the natural persons that they are subject to the use of the high-risk AI system. This information shall include the intended purpose and the type of decisions it makes. The deployer shall also inform the natural person about its right to an explanation referred to in Article 68c.</i></p>		AFME believes that EP Article 26(5a) is duplicable of Article 26(6a) and that only the latter should be retained.
EP 29a		<p><i>Article 29a</i></p> <p><i>Fundamental rights impact assessment for high-risk AI systems</i></p> <p><i>Prior to putting a high-risk AI system as defined in Article 6(2) into use, with the exception of AI systems intended to be used in area 2 of Annex III, deployers shall conduct an assessment of the systems' impact in the specific context of use. This assessment shall include, at a minimum, the following elements:</i></p> <p><i>(a) a clear outline of the intended purpose for which the system will be used;</i></p> <p><i>(b) a clear outline of the intended</i></p>		We do not support the EP's insertion of Article 29a as drafted. If it is to be retained, the scope should be narrowed to AI systems that fall within Annex III but have been evaluated by the provider as not posing a significant risk to health, safety or fundamental rights. Points (1)(d), and(1)(h) should be deleted, with point 1(j) amended. Reporting to supervisory authorities

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
		<p><i>geographic and temporal scope of the system's use;</i></p> <p><i>(c) categories of natural persons and groups likely to be affected by the use of the system;</i></p> <p><i>(d) verification that the use of the system is compliant with relevant Union and national law on fundamental rights;</i></p> <p><i>(e) the reasonably foreseeable impact on fundamental rights of putting the high risk AI system into use;</i></p> <p><i>(f) specific risks of harm likely to impact marginalised persons or vulnerable groups;</i></p> <p><i>(g) the reasonably foreseeable adverse impact of the use of the system on the environment;</i></p> <p><i>(h) a detailed plan as to how the harms and the negative impact on fundamental rights identified will be mitigated.</i></p> <p><i>(j) the governance system the deployer will put in place, including human oversight, complaint-handling and redress.</i></p> <p><i>2. If a detailed plan to mitigate the risks outlined in the course of the assessment outlined in paragraph 1 cannot be identified, the deployer shall refrain from putting the high-risk AI system into use and inform the provider and the National supervisory authority without undue delay. National supervisory authorities, pursuant to Articles 65 and 67, shall take this information into account when investigating systems which present a risk at national level.</i></p> <p><i>3. The obligation outlined under paragraph 1 applies for the first use of the high-risk AI system. The deployer</i></p>		<p>under paragraph 2 should be deleted. Notification to stakeholders in paragraph 4 and registration in paragraph 5 should also be deleted:</p> <p><i><u>Prior to putting a high-risk AI system as defined in Article 6(2) into use an AI system falling under one or more of the areas listed in Annex III that is not classified as high risk, according to Article 6 (2) of this Regulation, with the exception of AI systems intended to be used in area 2 of Annex III, deployers shall conduct an assessment of the systems' impact in the specific context of use. This assessment shall include, at a minimum, the following elements:</u></i></p> <p><i>(a) a clear outline of the intended purpose for which the system will be used;</i></p> <p><i>(b) a clear outline of the intended geographic and temporal scope of the system's use;</i></p> <p><i>(c) categories of natural persons and groups likely to be affected by the use of the system;</i></p>

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
		<p><i>may, in similar cases, draw back on previously conducted fundamental rights impact assessment or existing assessment carried out by providers. If, during the use of the high-risk AI system, the deployer considers that the criteria listed in paragraph 1 are not longer met, it shall conduct a new fundamental rights impact assessment.</i></p> <p><i>4. In the course of the impact assessment, the deployer, with the exception of SMEs, shall notify national supervisory authority and relevant stakeholders and shall, to best extent possible, involve representatives of the persons or groups of persons that are likely to be affected by the high-risk AI system, as identified in paragraph 1, including but not limited to: equality bodies, consumer protection agencies, social partners and data protection agencies, with a view to receiving input into the impact assessment. The deployer shall allow a period of six weeks for bodies to respond. SMEs may voluntarily apply the provisions laid down in this paragraph. In the case referred to in Article 47(1), public authorities may be exempted from this obligations.</i></p> <p><i>5. The deployer that is a public authority or an undertaking referred to in Article 51(1a) (b) shall publish a summary of the results of the impact assessment as part of the registration of use pursuant to their obligation under Article 51(2).</i></p> <p><i>6. Where the deployer is already required to carry out a data protection impact assessment under Article 35 of</i></p>		<p><i>(d) verification that the use of the system is compliant with relevant Union and national law on fundamental rights;</i></p> <p><i>(e) the reasonably foreseeable impact on fundamental rights of putting the <u>high-risk</u> AI system into use;</i></p> <p><i>(f) specific risks of harm likely to impact marginalised persons or vulnerable groups;</i></p> <p><i>(g) the reasonably foreseeable adverse impact of the use of the system on the environment;</i></p> <p><i>(h) a detailed plan as to how the harms and the negative impact on fundamental rights identified will be mitigated.</i></p> <p><i>(j) the governance system the deployer will put in place, <u>including human oversight, complaint-handling and redress.</u></i></p> <p><i>2. If a detailed plan to mitigate the risks outlined in the course of the assessment outlined in paragraph 1 cannot be identified, the deployer</i></p> <p><i>When assessing the systems' impact in the specific context of use, if the deployer identifies a</i></p>

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
		<p><i>Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, the fundamental rights impact assessment referred to in paragraph 1 shall be conducted in conjunction with the data protection impact assessment. The data protection impact assessment shall be published as an addendum.</i></p>		<p><u>significant risk of harm to the fundamental rights of natural persons, it shall refrain from putting the high-risk AI system into use and inform the provider, distributor, importer or authorized representatives, and the National supervisory authority without undue delay. National supervisory authorities, pursuant to Articles 65 and 67, shall take this information into account when investigating systems which present a risk at national level.</u></p> <p><u>3. The obligation outlined under paragraph 1 applies for the first use of the high-risk AI system. The deployer may, in similar cases, draw back on In case of high risk AI systems, for which the providers have already identified a significant risk of harm to the health, safety or fundamental rights of natural persons, according to article 6 (2) of this Regulation, this obligation may be considered as fulfilled by previously conducted fundamental rights impact assessment or existing assessment carried out by</u></p>

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
				<p><i>providers <u>without prejudice to the application of Articles 28, 29, and 52 of this Regulation.</u></i></p> <p><i>3a If, during the use of the high-risk AI system, the deployer considers that the criteria listed in paragraph 1 are not longer met, it shall conduct a new fundamental rights impact assessment.</i></p> <p><i>3b. Without prejudice to paragraphs 3 and 3a, a single assessment may address a set of similar AI systems that present similar risks and are listed in the same area of Annex III of this Regulation.</i></p> <p><i><u>4. In the course of the impact assessment, the deployer, with the exception of SMEs, shall notify national supervisory authority and relevant stakeholders and shall, to best extent possible, involve representatives of the persons or groups of persons that are likely to be affected by the high-risk AI system, as identified in paragraph 1, including but not limited</u></i></p>

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
				<p>to: equality bodies, consumer protection agencies, social partners and data protection agencies, with a view to receiving input into the impact assessment. The deployer shall allow a period of six weeks for bodies to respond. SMEs may voluntarily apply the provisions laid down in this paragraph. In the case referred to in Article 47(1), public authorities may be exempted from this obligations.</p> <p>5. The deployer that is a public authority or an undertaking referred to in Article 51(1a) (b) shall publish a summary of the results of the impact assessment as part of the registration of use pursuant to their obligation under Article 51(2).</p> <p>6. Where the deployer is already required to carry out a data protection impact assessment under Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, the fundamental rights impact assessment referred to in paragraph 1 shall be</p>

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
				<i>conducted in conjunction with the data protection impact assessment. The data protection impact assessment shall be published as an addendum.</i>
EP 51(1a) and (1b)		<p><i>1a. Before putting into service or using a high-risk AI system in accordance with Article 6(2), the following categories of deployers shall register the use of that AI system in the EU database referred to in Article 60:</i></p> <p><i>a) deployers who are public authorities or Union institutions, bodies, offices or agencies or deployers acting on their behalf</i></p> <p><i>b) deployers who are undertakings designated as a gatekeeper under Regulation 2022/1925;</i></p> <p><i>1b. Deployers who do not fall under subparagraph 1a. shall be entitled to voluntarily register the use of a high-risk AI system referred to in Article 6(2) in the EU database referred to in Article 60;</i></p>		AFME does not support the EP's insertion of Article 51(1b)
60(2a)		<p><i>2a. The data listed in Annex VIII, Section B, shall be entered into the EU database by the deployers who are or who act on behalf of public authorities or Union institutions, bodies, offices or agencies and by deployers who are undertakings referred to in Article 51(1a) and (1b).</i></p>		AFME does not support the EP's insertion of Article 51(1b) or its subsequent reference in Article 60(2a)
62(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	Providers and, where deployers have identified a serious incident, deployers of high risk AI systems placed on the Union market shall report any serious incident or any malfunctioning of those systems which constitutes a breach of obligations under Union law intended to protect fundamental rights to the <i>national supervisory</i>	[no change]	AFME does not support the EP's amendments to Article 62(1).

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
	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 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.	authority of the Member States where that incident or breach occurred. Such notification shall be made <i>without undue delay</i> after the provider, <i>or where applicable the deployer</i> , has established a causal link between the AI system and the incident or malfunctioning or the reasonable likelihood of such a link, and, in any event, not later than 15 days 72 hours (after the providers, <i>or, where applicable, the deployer</i> becomes aware of the serious incident or of the malfunctioning).		
63(4)	For AI systems placed on the market, put into service or used by financial institutions regulated by Union legislation on financial services, the market surveillance authority for the purposes of this Regulation shall be the relevant authority responsible for the financial supervision of those institutions under that legislation.	[no change]	For <i>high-risk</i> 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 <i>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, 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.</i>	AFME supports the Commission's drafting of Article 63(4), as retained by the EP.

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
			<i>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 that Regulation.</i>	
64(1-2)	<p>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.</p> <p>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.</p>	<p>1. <i>In the context of their activities, and upon reasoned request the national supervisory authority</i> shall be granted full access to the training, validation and testing datasets used by the provider, <i>or, where relevant, the deployer, that are relevant and strictly necessary for the purpose of its request</i> through application programming interfaces ('API') or other appropriate technical means and tools enabling remote access.</p> <p>2. Where necessary to assess the conformity of the high-risk AI system with the requirements set out in Title III, Chapter 2, <i>after all other reasonable ways to verify conformity including paragraph 1 have been exhausted and have proven to be insufficient</i>, and upon a reasoned request, the <i>national supervisory authority</i> shall be granted access to the training <i>and trained</i> models of the AI system, <i>including its relevant model parameters. All information in line with Article 70 obtained shall be treated as confidential information and shall be</i></p>	<p>1. [deleted]</p> <p>2. [deleted]</p>	AFME supports the Council's deletion of Article 64(1-2)

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
		<i>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.</i>		
69(1-2)	<p>1. The Commission and the Member States shall encourage and facilitate the drawing up of codes of conduct intended to foster the voluntary application to AI systems other than high-risk AI systems of the requirements set out in Title III, Chapter 2 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.</p> <p>2. The Commission and the Board shall encourage and facilitate the drawing up of codes of conduct intended to foster the voluntary application to AI systems of requirements related for example to environmental sustainability, 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.</p>	<p>1. The Commission, <i>the AI Office</i> and the Member States shall encourage and facilitate the drawing up of codes of conduct intended, <i>including where they are drawn up in order to demonstrate how AI systems respect the principles set out in Article 4a and can thereby be considered trustworthy</i>, to foster the voluntary application to AI systems other than high-risk AI systems of the requirements set out in Title III, Chapter 2 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.</p> <p>2. Codes of <i>conduct</i> intended to foster the voluntary <i>compliance with the principles underpinning trustworthy AI systems, shall, in particular:</i> <i>(a) aim for a sufficient level of AI literacy among their staff and other persons dealing with the operation and use of AI systems in order to observe such principles;</i> <i>(b) assess to what extent their AI systems may affect vulnerable persons or groups of persons, including children, the elderly, migrants and persons with disabilities or whether measures could be put in place in order to increase accessibility, or otherwise support such persons or groups of persons;</i> <i>(c) consider the way in which the use of their AI systems may have an impact or</i></p>	<p>1. The Commission, and the Member States shall facilitate the drawing up of codes of conduct intended to 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.</p> <p>2. The Commission and the Member States shall facilitate the drawing up of codes of conduct intended to encourage 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. <i>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.</i></p>	<p>AFME suggests amendments to the EP's drafting of Article 69(1-2) to focus on adherence to the spirit of compliance with the principles underpinning trustworthy AI systems:</p> <p>1. The Commission, <i>the AI Office</i> and the Member States shall encourage and facilitate the drawing up of codes of conduct intended, <i>including where they are drawn up so that AI systems other than high-risk embrace the spirit of the in-order to demonstrate how AI systems respect the principles set out in Article 4a and can thereby be considered trustworthy., to foster the voluntary application to AI systems other than high-risk AI systems of the requirements set out in Title III, Chapter 2 on the basis of technical specifications and solutions that are</i></p>

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
		<p><i>can increase diversity, gender balance and equality;</i></p> <p><i>(d) have regard to whether their AI systems can be used in a way that, directly or indirectly, may residually or significantly reinforce existing biases or inequalities;</i></p> <p><i>(e) reflect on the need and relevance of having in place diverse development teams in view of securing an inclusive design of their systems;</i></p> <p><i>(f) give careful consideration to whether their systems can have a negative societal impact, notably concerning political institutions and democratic processes;</i></p> <p><i>(g) evaluate how AI systems can contribute to environmental sustainability and in particular to the Union's commitments under the European Green Deal and the European Declaration on Digital Rights and Principles.</i></p>		<p><u>appropriate means of ensuring compliance with such requirements in light of the intended purpose of the systems.</u></p> <p>2. Codes of <i>conduct</i> intended to foster the voluntary <u>adherence to the spirit of compliance with the principles underpinning trustworthy AI systems, shall, in particular:...</u></p>
85	<p>1. This Regulation shall enter into force on the twentieth day following that of its publication in the <i>Official Journal of the European Union</i>.</p> <p>2. This Regulation shall apply from [24 months following the entering into force of the Regulation].</p> <p>3. By way of derogation from paragraph 2:</p> <p>(a) Title III, Chapter 4 and Title VI shall apply from [three months following the entry into force of this Regulation];</p> <p>(b) Article 71 shall apply from [twelve months following the</p>	[no change]	<p>1. This Regulation shall enter into force on the twentieth day following that of its publication in the <i>Official Journal of the European Union</i>.</p> <p>2. This Regulation shall apply from [36 months following the entering into force of the Regulation].</p> <p>3. By way of derogation from paragraph 2:</p> <p>(a) Title III, Chapter 4 and Title VI shall apply from [twelve months following the entry into force of this Regulation];</p> <p>(b) Article 71 shall apply from [twelve months following the entry into force of this Regulation].</p> <p>This Regulation shall be binding in its entirety and directly applicable in all Member States.</p>	<p>Noting our ongoing concern that the penalties will apply before the regulation applies, we support the Council's amendment to Article 85(2).</p>

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
	entry into force of this Regulation]. This Regulation shall be binding in its entirety and directly applicable in all Member States.			
Annex III (1)(1)	Biometric identification and categorisation of natural persons: (a) AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons;	Biometric <i>and biometrics-based systems</i> <i>(a)</i> AI systems intended to be used for biometric identification of natural persons, <i>with the exception of those mentioned in Article 5;</i> <i>(aa)</i> <i>AI systems intended to be used to make inferences about personal characteristics of natural persons on the basis of biometric or biometrics-based data, including emotion recognition systems, with the exception of those mentioned in Article 5;</i> <i>Point 1 shall not include AI systems intended to be used for biometric verification whose sole purpose is to confirm that a specific natural person is the person he or she claims to be.</i>	Biometrics: (a) Remote biometric identification systems.	AFME supports the EP amendments.
Annex III (1)(5)(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 for their own use;	AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score , <i>with the exception of AI systems used for the purpose of detecting financial fraud</i> the exception of AI systems put into service by small scale providers for their own use;	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 <i>providers that are micro and small-sized enterprises as defined in the Annex of Commission Recommendation 2003/361/EC</i> for their own use;	AFME supports the EP amendments.
Annex III (1)(6)(g)	AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data	AI systems intended to be used <i>by or on behalf of law enforcement authorities or by Union agencies, offices or bodies in support of law enforcement authorities</i> for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and	[deleted]	AFME supports the Council's deletion of this paragraph.

Article	Commission Proposal	EP Mandate	Council Mandate	AFME Comments
	sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data.	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.		