afme/
Finance for Europe

Association for Financial Markets in Europe

Consultation Responsea

Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)

6 August 2021

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to comment on **THE PROPOSAL FOR REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS** (the "Proposed Act"). AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

AFME is the European member of the Global Financial Markets Association (GFMA) a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association (ASIFMA) in Asia.

AFME is registered on the EU Transparency Register, registration number 65110063986-76.

We summarise below our high-level response to the consultation, which is followed by answers to the individual questions raised.

Executive Summary

AFME welcomes the opportunity to comment on the Proposed Act. Our response is set out in detail below, but we would particularly like to highlight the following key issues:

- General legislative principles: We believe that legislation should be technology-neutral and risk-based, noting the use of AI does not automatically generate greater risk but is one of several important considerations when assessing the degree of risk for any given application. It should focus on outcomes rather than specific techniques used, as this more effectively addresses underlying behaviours or practices and ensures that the legislation is future proof. It should also adopt a 'same activity, same risk, same regulation' approach that sets a level playing field between different actors, rather than imposing different requirements on firms performing the same activity.
- Application to regulated activities: Care must be taken to ensure that a horizontal initiative such as the Proposed Act does not duplicate existing requirements. Wholesale financial services firms are highly regulated, including in a range of areas that are relevant to the use of AI (such as consumer protection, model risk management, conduct risk, duty to clients, internal governance, third-party risk management, technology, outsourcing, operational resilience and data privacy). We encourage the consideration of a substituted compliance model wherever relevant requirements already exist.
- Supervision model for financial services: The proposed supervision model for credit institutions raises a number of questions, particularly as it relies on supervision by prudential authorities, whereas the issues addressed in the Proposed Act are more closely related to conduct. In addition, there is a risk of inconsistent supervision of the same issues across different types of firm and across countries and duplication between supervisors.

- Extraterritorial application: Consideration should be given to the extraterritorial application of the Proposed Act. For example, in cases where an AI application is hosted within the EU but used outside of the EU, without impacting EU clients. We suggest that this is called out as a specific exemption.
- In relation to the specific requirements in this proposed Act, we would highlight the following as of particular concern:
    - Article 3 on the Definition of AI: The chosen approach, to define an 'AI system' according to the technique that it uses, risks including systems that are not generally considered to be AI and resulting in a definition that is not future-proof.
    - Article 10 on Data Governance: The expectations placed on firms are unnecessarily burdensome and likely to be unachievable, for example, that data should be "free from errors".
    - Article 51 & 60 and Annex VIII on EU Database for Stand-alone High-Risk AI Systems: The requirement to make available 'Electronic instructions for use' raises concerns from a security perspective, as well as in terms of confidentially and commercial sensitivity.

Comments on the Proposed Act

General Comments

As a general principle, we believe that legislation should be technology-neutral, i.e. that (in this case) the use of AI should not increase the requirements (control, governance, transparency, etc.) per se. Legislation focusing on a particular technology (such as a specific AI application) is less effective, as it does not address underlying behaviours or practices, for which technology is simply a tool to perform. It should only be used where there are specific risks brought about by that technology that are not already covered by existing regulations, or where it is not possible to adjust or supplement the existing regulatory framework. This reflects a more risk-based approach, noting that the use of AI does not automatically generate greater risk but is one of several important considerations when assessing the degree of risk for any given application.

Given the speed of technological advances, technology-specific regulation will also struggle to maintain pace with developments in its use and risks, creating barriers to adopting new and innovative technologies.

Notwithstanding the above, we generally support the spirit of the recitals, which focuses on fostering the development, use and uptake of AI in the internal market that at the same time meets a high level of protection of public interests, such as health and safety, and the protection of fundamental rights, as recognised and protected by Union law[1].

We agree that the overall aim for AI as a technology is that it should be a tool for people and be a force for good in society, doing no harm. Accordingly, rules for AI affecting natural persons in the Union should therefore be human-centric, to promote trust that the technology is used in a way that is safe and compliant with the law, including with respect to fundamental rights.

We also share the common objective of harnessing the benefit of AI to improve predictions, optimise operations and resource allocation, personalise service delivery, support socially and environmentally beneficial outcomes and provide key competitive advantages to companies and the European economy.

We agree that it is important to have a balanced and proportionate horizontal regulatory approach to AI that is limited to the minimum requirements to address the risks linked to AI, without unduly constraining or

[1] Including the right to non-discrimination, data protection and privacy and the rights of the child (Recital 15)

hindering technological development or otherwise disproportionately increasing the cost of placing AI solutions on the market.

Finally, we request that the Commission considers the extraterritorial application of the Proposed Act. For example, in cases where an AI application is hosted within the EU but used outside of the EU, without impacting EU clients. We suggest that this is called out as a specific exemption.

Overall Structure of the Proposed Act

We welcome that the Proposed Act is a regulation, not a directive, as this will reduce the risk of divergence between Member States.

However, the structure of the Proposed Act seems relatively cumbersome and complex, with the main text accompanied by numerous annexes, several of which are subject to the management of a new agency ("European Artificial Intelligence Board"). The large number of authorities and stakeholders involved in the Proposed Act is also likely to increase the time required to implement and embed the requirements.

We also note that there should be a careful balance as to what is defined or scoped in as part of the Level 1 text, versus what is delegated to the Commission as part of Level 2. While the Level 1 text must naturally contain some key definitions, the process for amending or updating Level 1 is lengthier and may constrain the ability of the regulation to keep pace with developments in the technology or sector-specific requirements. In this respect, we refer again to our technology-neutrality comments above as this will reduce the need to make updates to the regulation over time.

Definition of Artificial Intelligence (Articles 3 and 4 / Annex I)

We appreciate that AI is a broad and complex term, which is often misused or misunderstood, and that definitions used in reports or academic papers attempt to describe AI as a concept and may, if used to develop policies, create uncertainty on the scope of the technologies subject to the proposed regulatory framework. The challenge is how to provide an accurate definition (e.g. avoiding the inclusion of other non-AI analytics technologies), future-proof (considering the pace of innovation in the field), and broadly harmonised with other major jurisdictions.

Although we understand that Annex I is intended to be read together with Article 3, we are still concerned by this approach, which appears to define an ‘AI system’ according to the technique that it uses. This approach is likely to capture non-AI methods (for example, statistical approaches and search and optimisation methods which have been in use in many applications across industries for some time and are generally not considered as AI). It will require more frequent updates as new AI techniques emerge that are not listed in Annex I (as is acknowledged in Article 4).

We would therefore appreciate the clarification that, to be qualified as an AI system, the software must (i) include one or more AI techniques listed in Annex I *and* (ii) produce outputs (content, forecasts, recommendations, decisions) that influence the environment with which they interact. Thus, on the other hand, software comprising an AI technique and producing outputs that do not autonomously influence the environment with which they interact would *not* enter into the definition of an AI system. In this case, to confirm the qualification as an AI system of software based on AI techniques and producing outputs, it is necessary to check whether these influence the environment with which they interact, and that consequently the stakeholders will have to identify the purpose and impact of the software used on their activities and the individuals concerned.

In our response[2] to the Commission's Inception Impact Assessment in September 2020, we suggested a revised definition of AI, based on the definition[3] provided by the Commission's High Level Expert Group (HLEG) on AI:

"Artificial intelligence (AI) systems are systems that act in the physical or digital world by perceiving their environment through data acquisition, interpreting the collected data, reasoning on the knowledge, or processing the information, derived from this data and identifying the best action(s) to take to achieve the given goal. AI systems may adapt themselves or their own algorithms by analysing how the environment is affected by previous actions, knowledge or data."

However, if there is no appetite to change the overall structure of the definition of AI system in the Proposed Act, then we would propose the following amendments:

- Article 3(1): Given the statement in Recital 6 that *"AI systems can be designed to operate with varying levels of autonomy"*, the concept of 'autonomy' should be included within the definition since it is a fundamental part of an AI system. We are interpreting autonomy to mean that the software is capable of inferring relationships from data, or by perceiving its environment. We suggest the following amendment to Article 3(1) *"'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, infer some or all the relationships relevant to the objectives from the data and generate outputs such as content, predictions, recommendations, or decisions without being explicitly programmed by humans and without being the results of so-called "deterministic and predictable" systems".* By this we mean that a system is said to be "deterministic" when it makes it possible to identify positively and unambiguously the causal relationships that determine the results it produces, and a system is considered to be "predictable" when it produces the expected results, which implies in particular that its results are not very sensitive to small variations in initial conditions; and

- Annex I: Point (b) should be removed, as this is broadly drafted and is likely to bring into scope applications that are not generally understood to be AI. For example, deterministic and fully predictable systems, located by nature "below" AI, such as Expert Systems (i.e. those based on knowledge bases and rules of inference).

- Annex I: Point (c) should also be removed for the same reasons. As currently drafted, point (c) would include any technique that involves estimation of unobservable or uncertain factors. For example, it is possible for basic queue optimisation for operational tasks to fall within this category, i.e. where a calculation is used for the mean and standard deviation of the time to close an individual task in order to allocate a new task based on recent work rates. We emphasise the importance of a risk-based approach, so as to not inadvertently broaden the scope of the regime to include the mere estimation of unobservable or uncertain factors.

In relation to Article 4 on amendments to Annex I, we would appreciate clarification that any updates would not be applied retroactively to bring in scope AI systems already in use.

<u>Other Definitions (Article 3)</u>

Article 3(2) defines 'provider' as a subject that *"…develops an AI system or that has an AI system developed…"*, however, the latter should be clarified. In particular, we note there is likely to be a difference between situations in which an 'off the shelf' system is purchased by a user, as opposed to when the user commissions a system, inputting into its technical specifications and may therefore be classed as a provider.

[2] https://www.afme.eu/Portals/0/DispatchFeaturedImages/200910_AI_IIA_Final.pdf
[3] https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

Article 3(4) sets out that a 'user' is defined as *"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"*. Similarly, in respect of importer and distributor, from a timing perspective, these are tied to points in time of 'puts into service' and 'making available on the market' which refer to 'use' in Articles 3(11) and 3(10). We are of the view that 'use' should be limited from a timing perspective. There may be instances where an AI system is in use, but for the purposes of using test examples to evaluate its effectiveness. While the AI system may be in 'use' as per the ordinary meaning of the word, it is not in 'use' in a context that would pose 'risks to the health and safety or fundamental rights of persons'.

Furthermore, we would appreciate guidance as to the level at which the 'user' should be defined. Some of the obligations upon users might mean that it would be inappropriate to define the 'user' at legal entity level. In such cases, the 'user' could be a function, team or even individual within the legal entity.

Under the definitions of 'user' and 'provider', it is possible for a provider to also be a user, for example, where a financial institution develops its own model for use within the firm or corporate group. In this respect, we would emphasise the need to ensure a proportionate approach to the requirements within the Act. For example, a user is required to 'monitor the operation' of the system per Article 29(4). However, as a provider, post-market monitoring obligations also apply under Article 61, whereby the provider should *"actively and systematically collect, document and analyse relevant data provided by users or collected through other sources on the performance of high-risk AI systems throughout their lifetime, and allow the provider to evaluate the continuous compliance of AI systems"*. These are duplicative. We would suggest that dual categorisation as a provider and a user is recognised, and that amendments are made to ensure no conflict or duplication of obligations in such cases.

We also suggest that the definition of 'deep fakes' which currently appears in Article 52 should be moved to Article 3 with the remaining definitions.

Finally, '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. We note that there may be instances where a firm purchases a 'High-Risk' AI system from a vendor (i.e. the firm is a user) and then, using its own data, performs training of the AI system. Periodic retraining can be a necessary part of ensuring an AI system remains accurate and/or is working as intended. However, this should not constitute a modification which is necessary to deem a user to become a provider. We, therefore, request that additional and periodic training of third-party AI systems is permitted to be undertaken by users without constituting substantial modification.

Definition of High Risk AI Systems (Article 6-7, Annex III)

First, we suggest that it would be more accurate to refer to these as "High-Risk AI Uses" or "High-Risk AI Applications", rather than "Systems". Similarly, the terms "unacceptable-risk AI systems", "low-risk AI systems" and "minimal-risk AI systems" should be replaced by, respectively, the terms "unacceptable-risk uses (of AI systems)", "low-risk uses (of AI systems)" and "minimal-risk uses (of AI systems). This would also support a more risk-based approach to the designation of what constitutes high-risk, better reflecting the fact that the use of AI does not automatically generate greater risk but is one of several important considerations when assessing the degree of risk for a given application (see also our comments below on Annex III in relation to employment, workers management and access to self-employment).

We request further detail as to how amendments to Annex III would be made. In particular, clarity on the process for input into any proposed changes by the private sector and the timeline by which compliance would be expected. A robust consultation process will be important where there is a risk of ambiguity in the scope of the activity intended to be designated as a High Risk.

In addition, the Proposed Act does not seem to provide for upgrades to the content of Annex II. We, therefore, suggest including in Article 7 the possibility for the Commission to adopt delegated acts in accordance with Article 73 to update the Union harmonisation legislation listed in Annex II.

Employment, Workers Management and Access to Self-employment

On the existing list of High Risk Systems in Annex III, we note that section 4 sets out those AI systems to be considered High-Risk on the basis that they are used for the purposes of 'Employment, workers management and access to self-employment'. The categories of high-risk AI are differentiated between pre-hiring use cases and post-hiring use cases. In a post-hiring context, use cases in scope will include AI intended to be used for:

- making decisions on promotion and termination of work-related contractual relationships; and
- task allocation and for monitoring and evaluating performance and behaviour of persons in such relationships.

Regarding this first category, we recommend that 'making decisions' should be limited to AI systems that make explicit recommendations as to 'promotion and termination'. We believe that the current drafting has the potential to scope in other use cases that may have a connection to 'promotion and termination' but are not used to make explicit recommendations or decisions that impact the individual in question. For example, to the extent that an AI system was to be used to make recruiting strategy changes, or to evaluate the difference between actual human decisions on 'promotion and termination' against formal promotion criteria, this could inadvertently be in scope based on the current drafting.

The scope of this first category should be appropriately read in light of the purpose of the regime, which is to 'ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values'.[4] As per the AI proposal, the EC note that in the context of promotion and termination, the use of AI should be high risk on the basis that it 'may appreciably impact future career prospects and livelihoods of these persons.'[5] On this basis, AI that is used in instances other than to make explicit recommendations for promotion and termination would not fall within the intention of the regime, as the AI system would not itself have an impact on future career prospects and livelihoods of these persons.

Similarly, regarding the second category of AI system used for 'task allocation', we are of the view that this should exclude pure operational task allocation that does not have an impact on 'future career prospects and livelihoods of these persons'. Other AI systems used to evaluate attrition or recommend mobility opportunities for employees should also be clarified as excluded from the requirements.

Access to and Enjoyment of Essential Private and Public Services and Benefits

We question the inclusion of 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"*. We note the concern in Recital 37 that the use of AI for this purpose may risk discrimination or limit a person's access to essential services. While we acknowledge the use of AI may make these risks more acute, we would like to highlight they are generally present whenever credit scoring is performed, regardless of the technology used. In fact, a well-built AI application could offer opportunities to improve the accuracy of the creditworthiness assessment, avoiding false positives that might lead to situations where clients could be unable to meet their financial obligations, and also helping more people to access financing (reducing the number of cases in which a credit is denied to a client who might deserve it).

[4] Page 3 – EU AI Proposal

[5] Page 26, Paragraph 36 – EU AI Proposal.

Furthermore, regulated financial services firms would be in breach of existing legislation relating to consumer protection (for example the EBA Guidelines on Loan Origination and Monitoring Section 4.3.4[6]) if they were to ignore or fail to mitigate such risks. It is therefore unclear what additional purpose is served by its inclusion in the Proposed Act, unless is it is intended to apply only to unregulated firms, in which case this should be made clear.

If 5(b) is to be retained, we suggest that (in line with our comments on category 4 above), it is restricted to cases in which AI is used to make explicit recommendations or decisions. We also suggest that, in line with Recital 37's reference to "access" to financial services, the system should be considered as high-risk only where it is used to evaluate the access to credit lending and is not the system put into service for phases following the initial disbursement of the loan.

In addition, we request that the exception included in the Annex 4, paragraph 5(b) "*with the exception of AI systems put into service by small scale providers for their own use*" is amended to be based not on scale but on the risks posed by providers for the clients.

Law Enforcement

In addition, we request clarification as to whether 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 sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data"* is intended to capture the use of AI in applications relating to Anti Money Laundering (AML) or Counter Terrorist Financing (CFT). Within financial services, AI is a useful AML/CFT tool for both financial services firms and regulators and is encouraged by the latter[7], so clarity that this wording does not cover its use by firms would be appreciated.

Application of the Proposed Act to Wholesale Financial Services

AFME supports that the Proposed Act takes a use case approach to defining High Risk AI Systems, rather than a blanket sectoral approach. This allows for the definition to focus specifically on AI usage that may pose health and safety risks or the risk of an adverse impact on fundamental rights, which are suitable measures for this purpose.

However, we would like to highlight again our preference that legislation should be technology-neutral and outcomes-focused. This is the approach that is currently taken within financial services, meaning that the Proposed Act would be a departure from this norm for financial services firms.

As a highly regulated industry, financial services firms are already under obligations relating to areas such as consumer protection, model risk management, conduct risk, duty to clients, internal governance, third-party risk management, technology, outsourcing, operational resilience and data privacy. Many of these will already mitigate the risks related to firms' AI use, throughout the lifecycle of any AI application, and will also drive firms' own initiatives to nurture the safe development of AI. These existing processes are tailored to the needs and specificities of financial services and (in relation to AI) to the different levels of risk of the AI applications. While the requirements of the Proposed Act are conceptually consistent with these existing requirements on financial services firms, their application would likely create duplication, complication, inconsistency and ultimately risk stifling innovation. This will likely add additional cost, complexity and uncertainty for firms, which could, in turn, limit the potential benefits for both firms and their clients. To mitigate this, to the extent that financial services firms are already regulated in the areas specified in the Proposed Act, compliance with

[6] https://www.eba.europa.eu/regulation-and-policy/credit-risk/guidelines-on-loan-origination-and-monitoring Paragraph 54 *"When using automated models for creditworthiness assessment and credit decision-making, institutions should understand the models used, and their methodology, input data, assumptions, limitations and outputs…"*

[7] We note, for example the joint statement by US Regulators in December 2018 encouraging banks to use innovative approaches to combat money-laundering, which cited the use of AI. See https://www.fincen.gov/news/news-releases/joint-statement-innovative-efforts-combat-money-laundering

those existing regulatory requirements should be deemed compliance with the requirements under the Proposed Act.

On the Proposed Act, we would like to request further clarity as to how the interaction with Directive 2013/36/EU (the Capital Requirements Directive, or "CRD") is envisaged and how supervision would work in practice. Although the broad application of CRD to credit institutions means that it would allow the Proposed Act to make use of an established supervision and authorisation model, CRD focuses on prudential matters, rather than those relating to conduct. CRD is therefore, from a subject perspective, not a natural fit with the purpose of the Proposed Act. Given that, as noted above, regulated financial services firms are also subject to a broad range of conduct legislation, including covering the subjects mentioned in the paragraph above, a formal substituted compliance model making use of existing conduct legislation would be more appropriate. If an assessment of conduct legislation highlighted any gaps with respect to the use of AI, these could then be dealt with separately, for example as part of this Proposed Act.

We understand that the EBA will release further guidance subject to completion of this Act. However, we have noticed a discrepancy between the various places in the Proposed Act where CRD integration is referenced:

- Articles 19, 61 etc, where CRD integration is only referred to in the specific case of creditworthiness and credit scoring (Annex III point 5(b)); compared to
- Articles 9, 17, 18, 20, 29 etc, where CRD integration does not appear to be limited and could therefore apply to all systems listed in Annex III.

We suggest that in the latter cases, a reference to point 5(b) of Annex III is inserted to make it clearer for financial services entities that the Commission is not intending to extend the material scope of CRD to non-credit-related use cases.

On a related note, care must be taken to ensure that the end state is not a fragmented supervision model for credit institutions, particularly between the EBA and Member State authorities, for example, in situations in which an issue emerges on a cross-border basis. We suggest that competent authority supervision is established on a subject-matter basis, for instance financial supervisors for creditworthiness and credit scoring, and national data protection authorities in the use of AI that involves processing of personal information, as outlined under General Data Protection Regulation (GDPR), for example.

Furthermore, to achieve harmonised application of this regulation across the EU, the opinions and recommendations issued by the European Artificial Intelligence Board on the application of this regulation should be binding for authorities of Member States, which should adopt them in their own acts.

In addition, we request clarification on what *"limited derogations"* is intended to mean in Recital 80 *"In order to avoid overlaps, limited derogations should also be envisaged in relation to the quality management system of providers and the monitoring obligation placed on users of high-risk AI systems to the extent that these apply to credit institutions regulated by Directive 2013/36/EU"*.

Regardless of the supervision model that is chosen for the final text of the Proposed Act, we would also like to highlight the importance of supporting supervisors in upskilling in this highly technical subject area. Supervisors must keep pace with their industries, where there is often already a high demand for technical skills, to provide effective oversight and challenge.

Finally, we would encourage the Commission to consider how the same high standards of governance and risk management can be ensured by financial markets participants who are not supervised under this Directive, in order to ensure a level playing field and to avoid unnecessary risk to clients or the wider industry from regulatory gaps. For example, the regulation could be amended so that all financial services firms involved in the activities referred in Annex III 5b are supervised by financial authorities, whereas non-financial subsidiaries of credit institutions not involved in activities in Annex III 5b are under the remit of the same National Competent Authorities (NCAs) as any other company providing AI systems for the same purpose.

Compliance with Requirements (Article 8)

We would appreciate further clarity as to how the reference to "intended purpose" in Article 8(2) (and elsewhere, for example, Articles 9(2)(b), 9(4), 9(7), 10(4), 10(5), 12(2) or 13 (3)(b)(i)) should be interpreted. It is unclear how this is intended to link to the definitions contained within Article 3 and how in practice, the intended purpose will qualify those requirements.

Data Governance (Article 10)

First, regarding the requirements in Article 10(2)(f) and (g), the Commission asks for i) examination in view of possible biases and for ii) identification of any possible data gaps or shortcomings. In respect of possible biases, while we agree that datasets may contain biases (real world data, for example, may be accurate and correct and yet reflet real world biases at the same time), it should not be assumed that this is inevitable and/or that complete removal of all bias is possible or a prerequisite for the use of such data within an AI application. Instead, such risks should be mitigated, taking into account any risks to clients, including via ongoing assessment of the application's outputs. Furthermore, the development of solutions for the complete removal of biases and shortcomings is an area of continued technical focus, but as yet, there is no consensus on the practicality of achieving this. In some instances, the approach is to assess for fairness in the outcomes of the AI, with unfair bias remediated at the outcome stage. In respect of "any" possible data gaps or shortcomings, the same concerns apply in that it should not be assumed that "addressing" all "data gaps" is possible. We, therefore, suggest that a similar risk-based approach should be permissible and suggest that "any" is removed to avoid potential confusion that all data gaps must be identified.

Second, we note that possible bias is not defined within the Act. Clarification is required as to whether bias in this context refers to existing concepts of prohibited discrimination in EU law.

Third, in relation to Article 10(3), it is unrealistic to expect data not to contain any errors. This is particularly concerning because the most burdensome fines for non-compliance are tied to the data and data governance requirements. Furthermore, it may disadvantage clients who are relatively 'data poor' or users who do not have access to the same hyperscale data capabilities as large incumbents or technology firms. We, therefore, request "*free from errors"* is deleted and replaced with "*take appropriate steps to identify the risk of errors and mitigate as appropriate"* which is a more realistic requirement. Furthermore, although we understand that this will naturally vary between use cases, further dialogue on how to interpret "appropriate statistical properties" and "relevant, representative…and complete" would be appreciated.

Fourth, as a general observation, we note that there is duplication between Articles 10(2)(3) and (4). It is likely that the issues canvassed as part of governance requirements in Article 10(2) would address the obligations in Articles 10(3) and 10(4). Consideration of whether the separate Articles 10(3) and 10(4) are needed is required, noting that subsuming these into Article 10(2) would remove duplication and allow for a more risk-based approach where firms can rely on the 'appropriateness' standard that Article 10(2) provides.

Transparency and Provision of Information to Users (Article 13)

We support the requirement that *"appropriate type and degree of transparency"* should be provided to users of high-risk AI systems. AFME's paper 'Artificial Intelligence and Machine Learning in Capital Markets: Considerations for a Broad Framework for Transparency'[8] set out how we consider that such transparency needs to be carefully tailored to individual stakeholder needs, rather than provided as 'one-size-fits-all'.

[8] https://www.afme.eu/Publications/Reports/Details/AITransparency

In relation to Article 13(3)(b)(ii), we do not think the 'user' must always know details of the accuracy, robustness, and cybersecurity referred to in Article 15. In particular, cybersecurity measures are sensitive within organizations and should not be shared with personnel unless there is a need to know such information. Furthermore, this information is likely to be overly technical to be useful. We request clarification that the level of information to be provided to users, where the users constitute individuals, is only to the extent necessary for such users to understand that accuracy, robustness and cybersecurity measures have been taken in accordance with the appropriate standards and to be aware of any limitations or risks. In this respect, we also note our comments on the definition of 'user' above, where further guidance would be helpful on the level at which the user should be defined.

Human Oversight (Article 14)

The lead into Article 14(4)(a) refers to the relevant human oversight being *"appropriate to the circumstances"* which we support as an approach; however, the inclusion of the word *"fully"* conflicts with this approach and should be removed.

Furthermore, given that it should be *"appropriate to the circumstances",* but Article 14(4) also sets out five separate ways in which this should occur, we would appreciate further guidance as to the admissible strategies and the cases in which one strategy should be preferred over others. For example, human oversight could be useful to support monitoring, but it may not be needed, or it may be impractical to expect it for every decision made by an AI system.

Quality Management Systems (Article 17)

Subject to our general comments on the use of CRD above, we also request clarity as to applying this Article to financial services firms. Article 17(3) states that the Article does not apply to firms regulated under CRD, but it is unclear whether this also covers the various other Articles cross-referenced in Article 17(1).

Obligations of Distributors, Importers, Users or any other Third-party (Article 28)

We note that the distributor is liable for all the obligations under this regulation, but that there is no provision for subcontractors or suppliers who may hold key information required by the distributor or user. We suggest that a clause is added specifying information (e.g. documentation, reports of audit) that a third-party AI provider should be required to provide to the user or distributor to enable them to assess their risks and fulfil their obligations.

As noted above in respect of "substantial modification" (referred to in Article 28(1)(c)) we request that this does not include additional and periodic training of third-party AI systems undertaken by users using their own data.

EU Database for Stand-alone High Risk AI Systems (Articles 51 and 60/Annex VIII)

On the existence of a public database of High Risk AI Systems, we are concerned that this could present security and business confidentiality risks (e.g. within financial services, AML/CFT risks), and request that an approach similar to the GDPR[9] Article 30 is considered, whereby lists internal to each company or organization can be made available to national supervisors.

While most of the details to be supplied to the database are administrative, we are concerned by the inclusion of item (11) 'Electronic instructions for use'. Detail to be included in such instructions extends to accuracy, robustness and cybersecurity in relation to the AI system. This requirement should be removed, or the scope clarified to ensure that firms are not being required to provide information that could introduce new vulnerabilities (such as cyber concerns) to the security of the AI system, or which could be confidential,

[9] Regulation (EU) 2016/679

proprietary and/or commercially sensitive. The availability of such information in the public domain may leave AI systems susceptible to manipulation and could mandate the publication of confidential information, eroding the incentive for providers to develop their own AI systems and potentially stifling the development of AI systems for use in the EU.

CE Marking of Conformity (Article 49)

We appreciate the aim of the Commission to build trust in AI-based services; the marking of conformity should contribute to this aim. However, we notice that the wording *"high risk system"*, as referred to in the Proposed Act, could become counterproductive and generate more fear than confidence if not adequately understood by citizens. For example, a client might prefer not to apply for a loan if the institution that performs creditworthiness analysis uses AI, because it is considered "high risk", and might choose instead another institution that does not use this technology. This would be to the detriment of the institutions trying to use more accurate data analysis technologies and the detriment of the clients, who could ultimately receive a worse service (e.g. have their loan rejected because of less accurate analysis).

There needs to be careful consideration of the information that will be shared with citizens so that they are not led to make an incorrect interpretation of the risks of these applications (e.g. with the conformity mark (Article 49 49), or with the publicly available list of high-risk applications registered in the Database for Stand-alone High-Risk AI Systems (Article 60(3)))..,. Firms could even be exposed to reputational risk by using AI in use cases expected for the financial sector, such as lending.

Further, it might also be difficult to explain to clients why certain use cases are high-risk while others are not and why non-high risk systems do not have a CE marking. Even more challenging to understand could be why the same use case might have a marking when using AI or not using this technology (e.g. which one would be "better" from a clients perspective, which technology would be promoted) These areas should be carefully considered to obtain the positive outcomes sought by the Proposed Act.

Transparency Obligations for Certain AI Systems (Article 52)

The transparency obligations for non-high risk AI should not apply to any AI system. However, these obligations should be linked to the potential for adverse harm to individuals or society, which the Recitals outline as the intended scope of the Proposed Act. We therefore suggest that in this context, 'natural person' should mean an individual acting in their personal capacity, not a person acting in a professional capacity/ on behalf of a legal entity, i.e. a 'legal person'.

We note the potential wide-reaching implications of this disclosure requirement. At present, this could potentially capture any AI system interacting where there is limited risk of 'impersonation or deception' as per recital 70 of the proposal (e.g. customised adverts, spell correction, spam prevention). We, therefore, recommend that this obligation is limited to instances where there is a clear potential risk of 'impersonation or deception'.

We would also appreciate additional clarity regarding the scope of transparency requirements concerning the use of AI systems with clients. We suggest that such transparency should only be required where the client is interacting directly with an AI application. For example, where an AI application is used to process the client's business or request, but there is no direct interaction, the transparency obligations under Article 52 should not apply.

Furthermore, we believe that this provision should be limited in its application when anonymity obligations prevent a provider from ascertaining whether the party with which the system is interacting is a natural person, a legal person or a machine. For example, in a capital markets context, AI systems may be built for the purposes of trading algorithms that trade on the open equities markets, where, by virtue of exchange anonymity, institutions may be unaware of the identity the other trading party.

AI Regulatory Sandboxes (Articles 53-55)

AFME welcomes the Proposed Act's support for regulatory sandboxes as a means for supporting the development and adoption of AI. However, the experience of our members in using regulatory sandboxes is that they function most effectively when they bring together a wide range of market participants, including incumbents, as well as start-ups and SMEs. They also require real-world data access to provide realistic scenarios to allow effective testing of projects. We would therefore caution against actions that prioritise start-ups and SMEs at the expense of existing market participants.

Reporting of Serious Incidents and of Malfunctioning (Article 62)

There may be existing notification obligations under existing or proposed Union law, e.g. the GDPR, DORA[10] or other financial services regulations. We request that the Proposed Act provides clarity on how the notification requirements under Article 62 will work in practice with these other requirements.

Access to Data and Documentation (Article 64)

We suggest that a provision is added to this Article that obliges third-party providers of AI systems to provide the required information to firms using their products to comply with this Article.

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. Accordingly, we request that Article 64 is clarified to permit exceptions.

In addition, to the extent that source code was exposed to a security breach, this presents 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. It would also be challenging to comply with where the model is sourced from a third party. Accordingly, we request that this provision is removed from Article 64.

Finally, we suggest that the reference to application programming interfaces (APIs) is removed and that the text refers only to *"appropriate technical means and tools"*. The requirement should remain technology-neutral rather than suggesting individual techniques. This will allow firms to determine the most appropriate and secure method of providing access.

Codes of Conduct (Article 69)

AFME is supportive of ensuring high standards in the use of AI within Europe and the move towards codes of conduct rather than the voluntary labelling system previously proposed. We believe that the object of trust should not be AI as a technology but that trust should be built up by the individual firm using a given AI application. This approach should be a focus of education about the use of AI in the EU, clearly explaining the benefits and dispelling the myths that may have arisen about the technology.

However, we suggest that further work will be needed on how a code of conduct could work in practice. While a very high-level code would bring little value, a very detailed code could risk becoming too specific to be broadly applicable and highly resource-intensive to audit against. There is also a risk that such codes could go beyond the original aim of the Proposed Act of safeguarding the fundamental rights of natural persons.

Similarly, there is a concern in relation to Article 69(1) that *"…codes of conduct [are] 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"*, given that the requirements for high-risk AI systems are likely to be disruptive if applied to low risk AI systems and impose disproportionate obligations. We suggest that the reference to Title III, Chapter 2 should

[10] The draft Digital Operational Resilience Act (DORA) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0595

be replaced with reference to any specific requirements that the Commission would like to see made more universally applicable. Alternatively, the Proposed Act should allow flexibility for how to pursue trustworthiness for non-high risk systems.

Furthermore, the suggestion in Article 69(3) that codes could be drawn up by individual providers of AI systems would result in a proliferation of codes that would again reduce the value to clients and end users.

There is also a concern about how to ensure that any codes remain truly voluntary in nature, rather than becoming a de facto market standard.

We would appreciate further clarity on how the Code of Conduct would relate to the High-Level Expert Group on AI (HLEG) Ethics Guidelines for Trustworthy AI. For example, the introduction to the Proposed Act notes that the guidelines were one of the inputs into this proposal, but is it envisaged that the development of a Code of Conduct would in effect supersede the guidelines.

Penalties (Article 71)

We appreciate that it will be necessary to place sufficient penalties for breach of the regulation to dissuade misconduct. We also support the inclusion of a list of factors in Article 71(6) to be taken into account when considering the penalty to be imposed. However, we suggest that an additional factor is added to consider the role of the entity in which the breach has taken place (i.e. distributor, user etc).

We are also concerned that the proposed calculation approach, which measures the fine in total worldwide annual turnover, would be disproportionate in cases where the breach occurs in a smaller entity or specific business unit of a global entity. If the fine is to be taken as a proportion of turnover, it would be more appropriate for this to be the turnover of the local entity within which the breach has been committed.

The highest penalty, 6% of worldwide annual turnover (or 30 million EUR) seems disproportionate to the potential for harm for use cases which do not fall within Article 5 (Prohibited AI Practices) and we would recommend that the scope of such penalty should be limited to breaches of Article 5 only. Moreover, we request more consistent alignment with GDPR penalty thresholds. The highest penalty under GDPR is 4 %, and this is for infringement of the provisions related to the core principles of GDPR, such as, for example, the legal basis for processing, including conditions for consent. Therefore, we request that the highest penalty be amended to a more proportionate number and at least aligned with the GDPR Article 83; however, in contrast to GDPR, it does not make sense to tie the % to worldwide turnover, for the reasons stated above.

The penalty for failing to provide accurate information is disproportionate. We request that such penalty be amended to a more proportionate number, for example, a fixed nominal fee of €100,000, with proportionality linked to % turnover for smaller firms.

There should be clarification in the Proposed Act that if there is a breach of the Proposed Act and a breach of other regulation, e.g. GDPR, or financial services regulation related to the same issue, regulators should co-ordinate and not be permitted to fine financial services firms disproportionately.

Finally, it would also be welcome if centralised guidance was provided to supervisory authorities regarding how to apply an appropriate penalty, to avoid fragmentation of approach between different authorities or Member States.

Entry into Force and Application (Article 85)

We believe that the Penalties (Article 71) should not be applied before the regulation itself applies. Moreover, we suggest deleting the following sentence *“Therefore the provisions on penalties should apply from (…)”* in Recital 88.

AFME Contacts

David Ostojitsch
Director, Technology and Operations
david.ostojitsch@afme.eu
+44 (0)20 3828 2761

Fiona Willis
Associate Director, Technology and Operations
fiona.willis@afme.eu
+44 (0)20 3828 2739

Tola Gbadebo
Associate Director, Technology and Operations
tola.gbadebo@afme.eu
+44 (0)20 3828 2734