27 September 2021

EBF_045345

EBF POSITION PAPER ON THE EC PROPOSAL FOR A REGULATON LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT)

Contents

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

I. Executive Summary

The European Banking Federation (EBF) welcomes the opportunity to comment on the European Commission's proposal for a Regulation for Artificial Intelligence (AI) and its **overall objectives to make the EU an "AI-friendly" environment, which encourages investment, aims to strengthens competitiveness and to ensure that AI systems respect fundamental rights and EU values.** However, EBF members are concerned that the proposed Regulation could, at the same time, **risk creating unjustified barriers or restrictions on the development of AI based business solutions, reduce research potential, render agile changes to existing applications difficult, and, ultimately, impact negatively on competitiveness.**

The Regulation needs to strike a balance between regulating high-risk AI use cases and supporting innovation (proportionate requirements, no unjustified barriers or restrictions, and no unnecessary administrative burden). It should rely as much as possible on the **principle of technological neutrality** i.e., AI is not an activity or use case in and of itself, and the mere fact that AI might be used should not increase the requirements (control, governance, transparency, etc.) *per se.* Such requirements should be based on particular risks of the use case and not on the underlying technology. This proportionate approach is missing from the text.

The Regulation should therefore be limited to requirements to address the risks based on the facts and circumstances, provided that they are not already covered by existing regulations, or that it is not possible to adjust or supplement the existing regulatory framework.

The banking and financial services sector is already subject to strong sectoral regulation and supervision, which ensures consumer protection, risk management and financial stability in all services provided to customers, regardless of whether those applications or services involve the use of technologies such as AI, including in the cases of creditworthiness assessment.

Coherence with existing requirements and the interaction of the proposed Regulation with the review of the Consumer Credit Directive[1] (CCD) and the European Banking Authority (EBA) Guidelines on Loan Origination and Monitoring[2] is crucial and needs to be outlined in the proposal**, as much of what is contained in the ex-ante proposals for high-risk AI systems is already addressed in these initiatives**. Duplication must be avoided. **Avoiding overlapping or conflicting requirements between the Regulation and the General Data Protection Regulation (GDPR) is likewise paramount.**

The supervision of this draft Regulation also **risks creating an unlevel playing field across different countries and industries if there is no consistency in supervisory expectations and practices among different national competent authorities**. These divergences could occur when the same high-risk AI application, such as creditworthiness assessment and credit scoring, is concerned since different entities might be supervised by different market surveillance authorities.

In order to ensure a level playing field for all industries in the application of the Regulation, the principle of ***'same activity, same risks, same rules'*****, must be taken into account**, while ensuring a well-coordinated and harmonized supervisory landscape for all market participants providing or using high-risk AI systems and maintaining a high

[1] European Commission, *Proposal for a Directive of the European Parliament and of the Council on Consumer Credits,* 30 June 2021, COM(2021) 347 final

[2] European Banking Authority, *Guidelines on Loan Origination and Monitoring,* 29 May 2020, EBA/GL/2020/06

level of consumer protection to ensure that consumers have confidence and trust in the use of AI.

We therefore welcome the objective of the Commission to bring legal clarity and foster the development of an ecosystem of trust in AI in Europe. This Regulation should be able to generate confidence in both citizens and companies offering AI-based services. **However we are concerned about how high-risk AI systems or products will be perceived by citizens and consumers.** The wording "high-risk AI system" could become counterproductive and create more rejection than confidence in those services compared to other equivalent services that may not be considered high-risk because they do not use artificial intelligence. This should be carefully considered when this rule comes into force. (see section B(d) for further details).

At the same time, **compliance with these requirements should be sufficient for companies to demonstrate to both regulators and users that they make an appropriate use of AI,** avoiding creating risks for citizens and in accordance with EU values.

- Complying with this Regulation should be sufficient to comply with the requirements to the use of AI introduced by other regulations such as the revised Consumer Credit Directive under discussion.
- It should also be sufficient proof for consumers of a fair and reliable use of AI.

Otherwise, companies will not have sufficient confidence to invest in the use and development of AI.

Ensuring legal clarity and trust in the proposal is therefore paramount, particularly regarding the **definition of AI, the scope, and supervision**.

Please find below **key messages on the Regulation on these three areas and detailed comments on the individual Articles in the Annex A**. A separate document with proposed amendments will follow.

II. Key messages on the definition of AI, scope, and supervision

A. The need for a more targeted definition of AI

i. Risks of an overly broad definition

The EBF believes that the existing definition of an AI System under Article 3 and the reference to Annex I related to AI techniques and approaches is **too broad and can include all types of systems or software applications which do not involve the same risks.** Given that the proposed definition will be the first definition of AI included in an EU Regulation and would be the reference for other potential rules referring to these technologies, we believe it is crucial for the Act to include **an accurate definition to ensure that requirements under the Regulation and potential future rulemaking that may reference the definition are fit for purpose.**

Depending on the definition, AI techniques and approaches can potentially encompass *any* possible application. Besides techniques that are generally considered to be AI, the current definition could include rule-based systems defined by humans or risk management techniques using standard formulas developed with statistical techniques. Since all these systems are applied to the Annex III high-risk use cases, this could result in an **extraordinary level of effort for managing these applications**, **despite these techniques having been applied for years and are generally not considered as genuine AI**, resulting in i) taking resources away from innovation and ii) managing effectively the true 'high risk' applications.

Looking at the financial sector, the suggested definition means that the use of traditional statistical processes, as used in credit institutions in part for decades, but at the latest since Basel II, leads to an undifferentiated categorisation as AI. Rather, the aspiration of a modern regulatory framework should be to enable companies to develop and deploy under risk-based considerations. **It is therefore surprising that rule-based procedures, which have been in use at banks for a long time and have been monitored and approved by the supervisory authorities, are now to be covered by the Regulation.** In the case of rule-based procedures, statistical procedures, mathematical functions or classification assignments, banks clearly specify, for example, which classification results are to be derived from certain data constellations. The risks of these methods are already adequately included in the financial institutions' risk management systems and addressed pursuant to their impact. **Including these methods in the definition raises significant uncertainties for banks as a result.**

ii. Recommendations

A **more targeted approach** for the definition of AI to **distinguish between different systems and the scope of applicability is needed.**

- Under Art 3., AI Systems are defined by the ability, for a given set of human-defined objectives, to ***generate*** outputs such as content, predictions, recommendations, or decisions which influence the environment with which the system interacts. **Generate is the crucial term in the text, one which unlocks the definition – but it remains unclear what systems fall in the scope?**

  To better focus the perimeter of AI systems, we would recommend to consider the difference between **data driven systems (systems that – given by human objectives, contexts, data and constraints – create the algorithm or the model *autonomously*, without human intervention)** and **model driven systems (systems that execute tasks defined and programmed by a human). The term "generate" should refer to "data driven systems".** Model driven systems should be excluded from the scope. This distinction would help to capture characteristics of the of the specific system e.g. the degree of autonomy, which, in our interpretation, the AI Act seems to be looking to capture.

- Looking at Annex I, letter c), it should be clarified that **only those techniques** are that are used to ***automatically and autonomously* adapt themselves** to new data or in other words, if such techniques have a self-learning character, are referred to. We would also recommend to amend **letter b) to exclude "expert systems"** which could also be designed using manually designed decision.
- **A clarification in the text on what "*system*" means, which is an additional layer of complexity on top of AI definition, is needed**. "Systems'' are subject to requirements and obligations. Take for example, **the case of a combination of components that constitute a system: how should this case be treated?** Each component as a system? What is expected in this case? And how should open-source systems be treated in this case? Clarification on requirements for open-source providers, to ensure this supports innovation rather than creating more complexity is needed. This is also relevant regarding the roles of 'providers' and 'users' of AI, and trialling / testing a bought system.
- Article 4 mentions that techniques listed in Annex I will be updated "*to market and technological developments on the basis of characteristics that are similar to the techniques and approaches listed therein*". **Again, based on the proposed definition, potentially any technique could be included in the scope of this regulation in the future.** There should be **clear criteria for including a new technique in the scope**, **and, in any case, in order to allow sufficient time for AI providers and users to comply with the regulation in the event that the list of techniques is modified**. We would propose a **grace period of 24 months**. Article 4 also provides for the possibility for the European Commission to adopt delegated acts to modify the list of techniques and approaches defined in Annex I. This means that the definition of AI may evolve, which is a source of legal uncertainty and may pose problems in the application of the risk-based approach.

Finally, the introduction of new techniques, in accordance with Art. 4, **should not have a retroactive effect for the systems already in place and follow the same rationale of Articles 83 and 85.**

B. Scope

a. <u>High Risk-AI Systems</u>

More guidance is needed to clearly identify when the use of AI systems **will be considered high risk and therefore subject to the requirements set out in this Regulation.** This is particularly important in light of firms innovating and developing new use cases that may not clearly fit into the categories set out in Annex III. Given the wide scope of the proposed definition, there is potential for uncertainty to inhibit innovation (and the risk of undue administrative burden and costs) if 'high risk' is applied too widely.

While we also recognize that it is paramount to promote a responsible approach to high-risk AI systems, **we have doubts if the extensive detailed requirements proposed regarding documentation, data governance, record keeping, testing and quality management systems, etc. are proportionate for all cases of high-risk AI applications**. Instead of taking a principle-based approach, these are sometimes very prescriptive (e.g., implementing detailed procedures instead of policies) and could limit the evolution of these technologies for the use cases in question.

We therefore believe that a proportionate approach to the different features of AI solutions should be followed and we appreciate Article 8(2) of the proposal which states that "*The <u>intended purpose</u> of the high-risk AI system and the risk management system shall be taken into account when ensuring compliance with those requirements*." To help firms navigate how this proportionality can be put into practice in light of the ‘intended purpose of the high-risk AI system and the risk management system’, the Commission could consider providing Recommendations. These could cover areas including how purpose and risk management should be taken into account in different requirements in order to have clarity and avoid divergences in supervisory expectations, particularly regarding the “thresholds” to be considered compliant, (e.g., regarding the quality management system), and provide practical examples of the approach.

If left unaddressed in the text, we are concerned that an excessively binding set of obligations will also **result in raising the barrier for using such AI systems**, **significantly increase development costs and time, as well as maintenance costs of such AI applications**, with a corresponding impact on internal processes, IT architectures and organizational settings and slow down innovation processes, when speed and efficiency are essential to compete in the digital economy.

Finally, as a general remark on the terminology, **we recommend to replace the term "*High-risk AI systems*" with the term "*High-risk applications of AI systems*", which is better suited to refer to what is actually covered by Annex III, i.e. a set of applications**. Following the same logic, the terms “unacceptable-risk AI systems”, “low-risk AI systems” and “minimal-risk AI systems” should be systematically replaced by, respectively, the terms “unacceptable-risk applications (of AI systems)”, “low-risk applications(of AI systems)” and “minimal-risk applications (of AI systems). We therefore wish to emphasize that **in a “risk-based approach”, it is the intended applications that are at risk, whatever the technologies used (AI systems or systems other than AI), and *not* AI systems themselves.**

b. AI systems used for creditworthiness assessment or credit scoring

It is important to underline, as a general remark, that creditworthiness assessments **have the objective to prevent harm and detriment to consumers**. Creditworthiness assessment that filters out borrowers who truly cannot afford the credit (*on legitimate bases for differentiation)* can be an essential step in avoiding irresponsible lending and should be considered as a first step in creating a sustainable credit market**. It is also useful to recall that banks have an obligation to control risks and that, as a result, the creditworthiness assessment must be carried out with discernment, with or without the help of AI**. This responsibility must be kept in mind when looking at the current framework.

i. Existing processes in the financial sector

Credit assessment in banks is already subject to a strict supervisory regime and banks have many years of experience with regards to granting credit to consumers and managing risks[3]**.** The competent authorities constantly monitor those procedures and this not only protects consumers and investors but also ensures financial stability.

Furthermore, under strict prudential rules, banks need to be able to measure, monitor and manage their sources of risk, including non-financial risk. **Model, technology, and information security risk management** are a part of this and encompass product approval processes that ensure risk management on products and services is performed,

[3] Examples of existing processes include:

- The revision of the CCD refers to the use of AI in Art. 18(6) *Where the creditworthiness assessment involves the use of profiling or other automated processing of personal data*. GDPR also introduces requirements to Automated individual decision-making, including profiling (Art. 22).
- EBA Guidelines on loan origination and monitoring introduce requirements regarding the use of automated models for creditworthiness assessment and credit decision-making (Section 4.3.4).
- The Mortgage Credit Directive (Directive 2014/17/EU) refers in Art. 18(5)(c) to decisions based on automated processing of data.

controlled, and monitored via the **"three lines of defense model"** (business, risk/compliance, internal audit). **This model sets a high standard in effective risk management and control and these principles apply irrespective of the techniques used and therefore encompass AI as well.**

As a result, we would like to stress once more the importance of **avoiding duplication of requirements and processes in the Regulation** and **ensuring that the scope of the creditworthiness assessment application referred to in Annex III is very precise** (see below for recommendations).

We would also like to flag that, by including credit scoring as high risk application, it is important to keep in mind that scoring systems are risk management based and do not aspire to make automated decisions by fitting a machine learning model to differentiate between defaulting and non-defaulting customers. Many different intermediate rating categories with specific default probabilities are used, not just two.

ii. Scope of credit worthiness assessment

1. *AI tools used in the wider credit process should be excluded*

In EBF members view, **the scope of the use case in Annex III 5(b) needs to be clarified as** the creditworthiness assessment process as a whole **can cover many kinds of systems in which the risk level varies. Not all the possible applications of AI systems introduce the same potential risk for a person's access to credit.**

The point on ***access*** is therefore key. Recital 37 specifies that creditworthiness and credit scoring are considered as high-risk "since they determine customers' ***access*** to financial resources or essential services such as housing, electricity and telecommunication services…". This **reference to the access should be explicitly clarified in the text of Annex III(5b)- only those systems used to evaluate the *access* to credit should be considered as high-risk. AI applications which are used in the wider credit process should be clearly excluded from the scope of the Regulation.** These include, for example:

- AI applications used in the valuation of collateral. These are rather a background tool in the process, and it does not affect a person's access to essential services.
- AI applications used in any phases following the initial disbursement of the loan. These have no impact on the decision of access to credit but are used for monitoring and internal process efficiency.
- AI applications focused on other process than credit (such as anti-fraud and anti-money laundering) that can be used as ancillary tools in the overall credit process.
- AI applications used for the marketing of credit products.

2. *The scope should not be limited to the financial sector*

The scope of this use case **should not be limited to the financial sector**. If credit-scoring is considered a high-risk use case than it **should be regulated for all providers, irrespective of the sector** (as with other use cases, e.g. AI systems intended to be used for recruitment or selection of natural persons). This intention, in our view, is already reflected in the draft Regulation with the **concept of "essential services**" in Recital 37 of the text and **should be clarified in the Annex.**

3. *The exemption for small scale providers should be removed*

The exemption included in Annex III 5(b) ("*with the exception of AI systems* ***put into service by small scale providers*** *for their own use*") **should be removed as any**

exemption should be based not in the scale but on the risks posed by providers for the customer. Maintaining the current scope would **most likely lead to an unlevel playing field and harm general trust in AI.** An ill-conceived AI system that is used by a small-scale provider is potential equally harmful towards the individual consumer as a large-scale provider. An unchecked AI based creditworthiness assessment will undermine trust in AI solutions in general and should be avoided.

What is meant by" their own use" is also unclear. Does it mean internal use (i.e., non-client facing) or as support to help make a human decision or something else? **Again, the risk towards the customer is not any different whether 'their own use' is done in the context of a small or large provider**.

4. *Additional clarifications*

We recommend to clarify how an algorithm will be treated when it is not initially designed for use in creditworthiness assessment (or indeed in any other high risk use cases) and is later repurposed (e.g. if a BigTech uses AI to analyse social media data for preliminary customer selection/screening and then markets credit to consumers on the basis of this information). This can be clarified in the text or, if necessary, through guidance.

c. Clarifications on other use cases

For high-risk AI Systems for biometric identification and categorization, laid down in Annex III, para1(a), **we recommend to clearly specify that neither the use of anti-fraud detection systems as used in remote client onboarding techniques**, **nor the use of biometric functionalities of a mobile device that allows a user to open an app or authenticate e.g. a payment fall into the scope of this provision**. Or at least, we would recommend to clarify what is meant by 'remote' or 'at a distance' in the regulation. Without this exclusion or specification, critical functions in financial services would be significantly impacted.

We also recommend specifying in Annex III that **AI systems used by compliance for counterterrorism and AML purposes are *not* interpreted as AI systems to predict the occurrence of potential crimes (Annex III, 6(e)).** There is also a concern among members that law enforcement authorities can unilaterally ask for data and model information, whether vendor or in house. This could raise the question of whether the bank's models / data are in fact 'used by law enforcement', particularly with regards to the data. A clear exclusion is therefore needed.

d. Consumer Education and Awareness

The draft Regulation rightly considers the risks to the consumer of certain high risk AI use cases; however, EBF members note that a consideration of potential, long term negative consequences is missing. Starting with the **wording of "high risk system"** – this could become counterproductive and generate more fear than confidence and trust in the consumer. **For example, a customer might prefer not to apply for a loan at an institution that performs creditworthiness analysis using AI because it is considered "high risk" and chooses instead another institution that does not use this technology.** A system classified as high-risk might be less acceptable by users than lower-risk systems, despite the former meeting much stricter requirements. **This would be to the detriment not only of the institutions trying to use more accurate data analysis technologies, but also to the detriment of consumers, who could ultimately receive a worse service (e.g. have their loan rejected because of less accurate analysis).**

The information that will be shared with citizens e.g. with the conformity mark (Art. 49), or with the publicly available list of high-risk applications registered in the Database for

Stand-Alone High-Risk AI Systems (Art. 60(3)) must be carefully considered so that citizens do not make a wrong interpretation of the risks of these applications that finally end up penalizing the use of this technology. Institutions could even be exposed to reputational risk by using AI in use cases as common for the financial sector as lending.

It might be also difficult to explain to customers why certain use cases are high-risk while others are not, and why non-high-risk systems do not have a CE marking.

We therefore recommend that the text **includes provisions for member states to promote measures that support customer education and awareness raising on the Regulation and the use of AI, its real capabilities and its benefits for their users in order to address doubts and possible myths that may exist.** AI provides great opportunities to deliver more suitable products and services to customers and to enhance their customer experience. It is also an opportunity to increase the efficiency of banking processes, and to enhance financial institutions risk analysis capabilities, strengthen security and risk management. Citizens need to understand these benefits, and that a service underpinned using AI can be improved for their benefit, either if they are based on AI systems that need to comply with this regulation (being designated as high-risk), or not.

C. Governance and Supervision

a. The European Artificial Intelligence Board

At national level, there are already different bodies and supervisory authorities acting in the digital field. Before designating a new authority to take charge of AI (The European Artificial Intelligence Board), we would recommend to:

- **Better define the missions of this Board in light of the challenges of international competitiveness, innovation, and data processing** (personal or industrial).
- **Clarify the role of existing authorities** and how they would fit within this new constellation. For example, what will be the **role of Data Protection Authorities at national level and the role of the EDPB at European level when it comes to use of personal data in AI**.
- **Involve a wider stakeholder group in the work of the Board** to contribute to a more balanced view on AI developments, particularly when it comes to any potential additions to the Annex.

b. Supervision and the need for a level playing field

From the point of EBF members, there are two angles to consider on this topic – i) supervision for credit institutions activities and the ii) need for a level playing field.

i. Supervision for credit institution activities

We welcome the designation of financial authorities as Competent Authorities for credit institutions' activities (Art.63(4)) since this would simplify banks' compliance and supervision obligations. With regards to use case 5(b) under Annex III, first we would like to underline the **need to ensure coherence with the proposal for a revision of the Consumer Credit Directive[4] (CCD), as well as the need to make a clear distinction between the two proposals**.

The AI Act aims *to lay down harmonised rules for the* ***placing on the market, the putting into services, and the use of AI systems*** *in the Union and* ***specific requirements for high risk AI systems*** *and* ***obligations for operators of such***

[4] European Commission, *Proposal for a Directive of the European Parliament and of the Council on Consumer Credits,* 30 June 2021, COM(2021) 347 final

systems (Art. 1(a)& (c)) while the CCD establishes the ***entire* harmonised framework for granting consumer credit** – going beyond the scope of the AI Act when it comes to the creditworthiness/credit scoring use case and covering all aspects of consumer protection. For example, Recital 48 of the CCD provides for transparency and contest right as well as human intervention in case of automated decisions. This goes beyond the requirements of the AI regulation in terms of safeguarding consumer rights.

In light of this, **there needs to be a clear delineation of the scope in both proposals – the AI Act and the CCD- to provide legal certainty for consumers and firms. Alignment with the EBA Guidelines on loan origination and monitoring is also key.**

Second, we would welcome a clarification on how supervision with regards to the AI Act **would materialize in jurisdictions with different supervisory models** for credit institutions, for example, those jurisdictions with a 'twin peaks' model. We note that the expertise for considering such matters as human rights, accuracy and 'bias' in the context of creditworthiness assessment may lie with the market conduct authority more than the prudential authorities, where these are separate bodies.

ii. ***Ensuring a Level Playing Field***

While the designation of financial authorities as competent authorities for credit institutions activities under the Regulation is welcome, it also **raises the risk of fragmentation in supervision, as non-financial firms providing or using the same high-risk AI systems as financial entities would be subject to the oversight of authorities that would have their own interpretation and approach to this Regulation, which could mean a less stringent framework.** This is especially concerning in the case of use case 5(b) in Annex III on creditworthiness assessment, where the situation would lead to two supervisors on the landscape: the prudential regulator for banks, and the lead AI supervisor for non-licensed firms.

To ensure that the "same activity, same risks, same rules" principle is applied, and to reduce the risk of unbalanced competition, the EBF proposes to amend the Regulation so that **all firms involved in the activities referred in Annex III 5(b) are supervised by financial authorities with regard to such applications** . If this is not possible, **it is necessary to identify guidelines or criteria for each authority to follow and comply with for a harmonised interpretation and application of the AI Regulation, not only with regards to use case 5(b), but all high-risk use cases** in order to avoid the risks of and that certain actors are subject to more stringent requirements in one member state than another.

For example, including the conformity assessment as part of the Supervisory Review and Evaluation Process (SREP) of credit institutions, as suggested in Arts. 19(2) and 43(2) **should not increase supervisory expectations nor create additional requirements for credit institutions with regards the use of AI**. According to Art. 16(j) providers shall "*upon request of a national competent authority, demonstrate the conformity of the high-risk AI system with the requirements set out in Chapter 2*". Being part of the SREP should not increase the expectations for credit institutions to demonstrate conformity with this Regulation. **This should be clearly stated in the text**. Otherwise, the same requirements should apply to any other non-credit institution. In addition, it should be noted **that the timing of incorporating these requirements into supervision will also be key to preserving competition among banks and other firms** should it become necessary to set up AI supervisors for non-credit institutions and unlicensed firms.

Also, currently there is a risk that a subsidiary of a banking group, which uses or provides high-risk AI systems, but is otherwise not involved in the bank's credit business, may fall under prudential regulation and supervision. For example, this can be case if regulation is applied on the consolidated level (or even below the consolidated level), and consequently this subsidiary would also be supervised by financial authorities. This could potentially create an unlevel playing field with respect to their competitors not having links with financial institutions.

In order to reduce the above risks, **coordination between different authorities (particularly in light of the existing sectoral and horizontal regulatory framework) is crucial. It should be ensured that the criteria of the authority with more expertise on each use case prevails as well adequate resources and expertise in organizing the supervisory framework are allocated**. The implementation of an organisation chart (e.g. RACI) in order to describe the prerogatives of the various competent authorities would help to provide clarity. In addition**, making the opinions, and recommendations on the implementation of this Regulation issued by the European Artificial Intelligence Board binding for authorities of members states that should adopt them in their own acts could be another way to address fragmentation**.

D. Conclusion

European banks recognize the importance and responsibility of ensuring risk management and consumer protection for all services provided to customers, including those applications that involve the use of AI. We would therefore like to recall the principle of technological neutrality and that any regulatory requirements should be based on risk per use case and not on technology.

The financial sector is not starting from a blank page when it comes to AI. In this regard, it is crucial that the European Commission’s proposed Regulation **is coherent with existing sectoral, financial regulation and horizontal regulation, notably the GDPR and does not lead to a duplication of requirements**. It must not pose a barrier to innovation and widespread adoption of AI through prescriptive requirements or result in an unlevel playing field, where some actors providing the same use cases are subject to stricter requirements than others. Furthermore, the ‘high-risk’ categorisation of certain use cases, and those who will fall in and out of those, risks a counterproductive outcome –**a result where consumers choose products which are not designated high risk, but subject to lower requirements, to their detriment**. If Europe is to promote the adoption of trustworthy AI and become a leader globally, these shortcomings must be addressed.

III. ANNEX 1- DETAILED COMMENTS

As a general remark, the EBF notes that some concepts (e.g., 'foreseeable risks', 'reasonably foreseeable misuse', 'generally acknowledged state of the art') are vague and some obligations refer to other Union laws intended to protect fundamental rights. **This could create legal uncertainty that should be removed in the final text by avoiding the inclusion of terms and legal references that could be interpreted differently by providers, users, and authorities.** In those cases where some legal uncertainty cannot be removed in the final text, the Commission should develop guidance or recommendations to ensure supervisory expectations are aligned and understood by providers and users having to meet the legal requirements.

TITLE I: General Provisions

- **Article 2 (1c)**: The scope of the proposal regarding providers and users of an AI system located outside the EU risks creating legal uncertainty. Recital 11 states that "*certain AI systems should fall within the scope of this Regulation even when they are neither placed on the market, nor put into service, nor used in the Union*". This approach is too broad, and risks confusion for all the actors in the AI value chain. **This provision should be amended to focus more clearly on the 'evasion' activity that we understand the Commission is seeking to avoid**. Furthermore, this Article includes the scenario where the AI provider and users are outside the EU, but the 'output' is used in the EU, **without defining 'output'**. We recommend to expand the examples of 'output' in Article 3(1), to clarify this provision, and to include a definition of the term in the text.
- **Article 3(2):** The term 'provider' is defined as a subject that "*develops an AI system or that has an AI system developed* (…)". **The phrase "has an AI system developed" is vague and requires further clarification.** We believe it is intended to refer to where a firm *orders / secures the development* of an AI system. However, it might also be read as referring to where a firm *possesses* an AI system, (would this refer to titles, rights, licence, property, etc.?) In addition, it **should be clarified that 'developing' an AI system does not include simply training it**, unless this amounts to a 'substantial modification' (see also comments below).
- **Article 3 (2) & (4)**: Regarding the roles of 'providers' and 'users' of AI, it is highly likely that they will often be the same firm. This could lead to a duplication of obligations, (e.g. monitoring under Art.29(4), or under Art.61). **The proposal should recognise that a firm can play both roles and allow compliance in a proportionate fashion by removing duplicate requirements.**

  In cases where a user acquires an AI system, it might need to trial / test the system in order to evaluate its effectiveness. **In this context, the AI system would be**

'in use' but would not pose 'risks to the health and safety or fundamental rights of persons'. The EBF is of the view **that this case should be excluded from the scope of the requirements**, e.g. via amendment to Article 3(4). (Similar changes to Article 3(10) and 3(11) may also be needed to clarify that testing does not trigger obligations). Otherwise, the inclusion could entail implementing processes and procedures not only for the identified AI use cases but also for cases where a bank simply decides to test an AI solution, without actually implementing it. This risks incurring disproportionate costs and time.

- **Article 3(23): 'Substantial modification'** is defined to include *any change* to the AI system which is changed in a way that would affect compliance with Title III, Chapter 2. **However, the AI user will often have to do supplementary and periodic training of an AI algorithm using its own data to ensure the system remains accurate and/or is working as intended.** If this user data does not meet the data requirements as currently drafted (please see comments below), this could cause non-compliance with Title III, Chapter 2. We recommend that Article 3(23) clarifies that this kind of supplementary and periodic training **does not amount to a 'substantial modification' (i.e. the user does not become a provider of AI)**, though a requirement similar to Article 29(3) should be added in respect of AI users' training data. Also, the exclusion in Article 43(4) for changes that are 'pre-determined by the provider' should probably be included in Article 3(23) as well / instead.

- **Article 3(32):** In the definitions "input data" is described as "*data provided to or directly acquired by an AI system on the basis of which the system produces an output*". How should this be interpreted/linked to target data? This is not used in Article 10 when it comes to relevance and representativeness. We also recommend that the definition of "deep fakes", as described in Article 52(3), should also be included in Article 3.

TITLE II: Prohibited Artificial Intelligence practices

- **Article 5**: The EBF is of the view that the **definition of prohibited practices may appear somehow generic** and **lead to multiple interpretations or misinterpretations about the perimeter of prohibited practices**. The criteria that permit the identification of prohibited practices should clarify the way to determine if a system built for commercial solicitations as its intended purpose is prohibited or not.

TITLE III: High-Risk AI Systems

- **Article 7**: While the EBF understands the possible need for updating the list of high-risk use cases under Annex III, this can be problematic from the predictability point of view. It is paramount that there are **sufficiently long transition periods if new high risk use cases are introduced later on**. **Article 7 should be strict enough to ensure that the list is not updated without real justification, and the threshold should be sufficiently high**. It should also be considered whether additional elements need to be taken into account in the assessment of whether an AI system is added to the Annex. Clarifications on how the principles of better regulation, transparency and the need for impact assessments are taken into account in the context of delegated acts would also be welcome.

  We also note that the proposal does not provide the possibility to update the content of Annex II in case new AI systems are included under Annex III. As the list of Union harmonization legislation may be affected from relevant updates in the latter, we 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.

- **Article 7(2):** Regarding the possibility for the Commission to adopt delegated acts to update the list in Annex III by adding high-risk AI systems, we consider the **criteria listed in this provision too broad**, which is **a source of legal uncertainty** that could prevent companies from developing innovative AI solutions due to the unpredictable evolution of the scope in the coming years. **Explicit provisions should be introduced for stakeholder involvement in any future work to update the list.** We would also recommend to specify what should be understood by "harm" or "adverse impact".

- **Article 9**: It is important to specify if there is any expectation to manage the processes aimed at ensuring the compliance of the Regulation via a "cross-functional" rather than a dedicated team in the case of risk management systems.

  More broadly, Articles 9, 19 and 43 require AI actors to conduct risk and compliance analysis with all applicable legislation. **The relationship between these obligations and the risk analysis provided for in other texts, e.g. in Article 35 of the GDPR, should be clarified.** To this end, it will be necessary to specify the role of the Data Protection Officers on AI issues.

- **Article 10**: It could be difficult to distinguish between personal and non-personal data due to the overall complexity of AI systems. With reference to this, we recall that Article 2 paragraph 2, Regulation (EU) 2018/1807[5], as well as "Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union[6]" states that: "*(…) in a case of a dataset composed of both personal and non-personal data: (i) the Free Flow of Non-Personal Data Regulation applies to the non-personal data part of the dataset; (ii) the General Data Protection Regulation's free flow provision 26 applies to the personal data part of the dataset; and (iii) if the non-personal data part and the personal data parts are 'inextricably linked', the data protection rights and obligations stemming from the General Data Protection Regulation fully apply to the whole mixed dataset, also when personal data represent only a small part of the dataset*". Therefore, we encourage the EC to **avoid duplications and inconsistencies with the abovementioned Regulation and Guidance.**

- **Article 10 (2f, g)**: The proposal asks for *i) examination in view of possible biases and for ii) identification of any possible data gaps or shortcomings.* These requirements seem to demand providers to avoid bias amplification on one side, without giving any practical clue on how to technically achieve this result on the other side. **This is worrying, particularly as the issue of how to achieve such a result is still widely discussed and largely unsolved, even at the scientific level**. Instead, such risks should be mitigated, taking into account any risks to clients, including via ongoing assessment of the AI system's outputs.

  Similarly, in respect of sub-paragraph (g), it may not be practically possible to a "address" all possible data gaps (as implied by the word "any"). 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**. We also note that possible bias is not defined within the Act. This is a complex issue, **with considerations that will likely vary between different use cases.** Guidance will require careful discussion with sectoral regulators in due course in order to avoid unintentional consequences.

[5] Regulation 2018/1807 of The European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union

[6] Communication from the Commission to the Parliament and the Council, *Guidance on a framework for the free flow of non-personal data in the European Union,* 29 May 2019, p.9

- **Article 10 (3)**: The **requirement for training, validation, and testing data to be free of errors and complete is disproportionate and impractical:**
    - It is impossible to guarantee the absence of errors in the data sets used in the development process of systems.
    - The concept of no errors is contrary to the principle of AI which conceptually incorporates this ability to reproduce human analysis. Every sizable dataset will include some degree of errors.

  We therefore recommend to:

    - Focus on **"sufficiently free of errors to not materially affect the desired performance of the AI system" or "take appropriate steps to mitigate the risk of errors".** These requirements must also be taken together with Art.8 and 9, **looking at the "intended purpose of the AI system and the risk management system",** which will help to understand what it means to be "sufficiently free of errors" in that context.
    - Most AI applications run on observational data, not on statistically constructed sample data. This could make it very difficult to match the requested requirements, due to unreachable data properties. We would suggest adding a distinction and specifying that, in case of observational data, a common approach on data requirements is defined together with regulators.
    - **The term "representative" requires further clarification,** specifically about whether it is related to protected groups/classes of people or to the use case.
    - The term "complete" seems as an absolute measure as well. It is common to have datapoints that are not available for all input rows. This is not always a problem for the performance / risk or application of an AI system. Similarly we believe that it should be evaluated as **"sufficiently complete to not materially affect the desired performance of the AI system".** The filling of a data field is not necessarily required, because already the indication or non-indication of a piece of information in interaction with further information contributes to the improvement of the performance in many cases. The omission of such data because of the completeness requirement would lead to a deterioration in performance. As a result, higher risk costs would have to be borne by borrowers via the lending rate or a more restrictive acceptance policy would have to be expected, which would tend to exclude borrowers with a somewhat weaker credit scoring from being granted a loan. This would not be in the interest of customers.
    - As a general observation**, we note that there seems to be a 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 would be welcome, 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.**
- **Article 10(6): The requirements under this article should be considered fulfilled by complying with the Capital Requirements Directive (CRD)[7] governance requirements.** We note that the proposal already provides for some explicit derogations for credit institutions (e.g. Arts. 17(3) Art.29(4)).

[7] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms

- **Article 12:** The requirement that high-risk AI systems shall be designed and developed with capabilities enabling the automatic recording of events ('logs') while the high-risk AI systems is operating is **too prescriptive**. The EBF is of the view that there are other techniques less onerous in terms of processing and storage that can ensure appropriate record-keeping capacities and reproducibility of the system and therefore **automatic logs should be optional**.
- **Article 13 (2)**: The electronic instructions for use include the characteristics, capabilities, and limitations of performance of the high-risk AI system. As the EU Database for Standalone High-Risk AI systems (Art. 60) will be public such information, if provided in detail, would **risk making the models susceptible to manipulation and 'gaming',** and risks exposing confidential information, impacting the incentive to innovate by banks. The rules around disclosure of information **should allow for firms to take a proportionate approach, to manage these risks.**
- **Article 14**: Human oversight is outlined in the text **in five significantly different ways**, while also indicating that this should be followed "as appropriate to the circumstances". **Clarification is needed about the admissible strategies and the cases in which one strategy should be preferred over others**. Human-oversight could be useful to support the monitoring, but it seems impractical to expect it for every decision made by an AI system.

  Individuals to whom human oversight is assigned must be able to 'fully understand' the capacities and limitations of the high-risk AI system and be able to 'correctly 'interpret the high-risk AI system's output. We note that the terminologies underlined above, 'correctly' and 'fully understand' suggest that a binary determination can be made under the respective allocated tasks, while in practice there can be uncertainty. For example, where a CV screening AI system is built by a third-party provider, such a system might produce a result indicating that a candidate is a 51% match for the position concerned; it would be difficult to ascertain whether a 'correct' interpretation can be taken from such a result. **So the human oversight obligations should have regard for the relevant use case circumstances, including the nature of the AI system result and whether it is appropriate to set a binary standard of 'correctness'.**
- **Article 26:** The definition of high-risk AI systems expressly includes AI components, but it is necessary to **clearly articulate the responsibilities of each player**, in particular when AI components are proposed. **Indeed, in terms of liability and obligations, how would one deal with AI components built by suppliers, but assembled by the user?** Under Article 26, will the importer of these components similarly have to ensure that the compliance analysis have been carried out by the supplier? The supplier of an AI component must be able to document elements not only on the performance of its component but also on the validation of the methods used.
- **Articles 27, 28, 29**: **The responsibilities and the liabilities of the different actors "in the AI value chain" must be clear and precise**. For instance, if a bank's (non-AI) product or service is based -partly or as a whole- on data gathered from interfaces of other actors (private or public, EU or non-EU), it is not clear to what extent the bank is responsible for the AI system "behind the interface". The AI regulation contains provisions, e.g. on the role of the distributor, but there is **still uncertainty as to how responsibilities are divided in a situation where an AI system is not actually made available on the market but could be part of a value chain somewhere in the background,** especially given the extraterritorial applicability of AI 'outputs' generated abroad but used within the EU (see comments above). Additionally, the value chain could be even longer.
- **Article 28**: Any distributer, importer, user or other third party is considered a provider if they "make a substantial modification". We **recommend to further**

specify what constitutes a "substantial modification". Many market AI systems need to be adjusted before being put into service and **a too generic definition of "substantial modification" could lead to always identifying users as providers, leading to a disproportionate outcome**. (Please see comments and suggestions above on the definition of 'substantial modification').

- **Article 49**: Rather than prioritising a "one size fits all" solution across all industries, (including financial services) with CE marking, **any resulting trust or conformity signalling requirements should be meaningful, easily understandable and meet user needs first and foremost, and align with already established norms and requirements of sectoral supervisory authorities**. Global voluntary industry-driven standards (created by technical experts) enable commonality and reduce fragmentation on technical aspects, quality management, governance, and risk management of AI to help industry, which is operating in a global market, to adopt AI. Global standards are designed to be flexible and to foster, not hinder innovation by being too prescriptive, while also helping to raise the bar on transparency, privacy, cybersecurity, safety, and resilience. It is important that CE markings do not undermine these efforts.

  The process of obtaining a CE marking is not described in detail in the proposal. It would be problematic in case it takes a long time and slows down the market entry for administrative reasons. For the use case of AI systems used for creditworthiness assessment and credit scoring, it is not clear where to place the CE marking.

- **Article 51**: The EBF believes that the transparency requirements for the register (Annex VIII) should **not hinder the use of fraud detection systems**, e.g. for AML purposes. Far reaching transparency requirements (e.g. for high-risk AI-systems in the future) for fraud detection systems are a concern in the effective use of such systems.

  In the interest of Intellectual Property rights, **access to the source code of AI systems by supervisors should be limited**.

  Furthermore, AI systems are typically not static, and some state-of-the-art systems undergo continuous learning and transformations. Given that the procedure to approve models/update the database is not yet clear, we suggest including a **distinction between new models and models to be updated**. A **simplified process with a periodical update of the database in case of already approved AI systems** which are just updates/modified would be preferable in order to avoid slowing down the usage of updated models.

Title IV: Transparency Obligations for Certain AI Systems

- **Article 52**: The current text could capture a wide range of use cases, such as anything which displays customised adverts or spam prevention (given the AI definition and the inclusion of generation of 'content'). If there are too many notifications, they will eventually lose their effectiveness. **The EBF suggests further targeting these rules on situations where there is a high risk of impersonation or deception.** Additional clarity would also be welcome as regards transparency requirements in relation to the use of AI systems with clients. **Transparency should only be required where the client is interacting directly with an AI application as set in Article 52 and not be required when there is no direct interaction, such as for processing the client's business or request.**

  Also, this obligation may need to be adjusted to cater for those situations where the parties involved are acting in their professional capacity, and, therefore, it can be assumed that they are aware of the possibility of interacting with an AI system or, where anonymity obligations exist, that prevent a firm from ascertaining whether the party that the system is interacting with is a natural or legal person.

Title V: Measures in Support of Innovation

- **Article 53**: While we consider it very important to make sure AI is safe, unbiased, fair, and secure, the proposal should at the same time sufficiently support room for experimentation and testing, also with regard to global competition in the field of AI. While the Commission aims to reduce the burden for development and exploration of new AI systems, while keeping the bar high for those in production, **the current sandbox proposal is not sufficiently suited for this purpose**. Instead, **it seems more suited for larger and far-stretching implementations** (e.g. an experiment with faceID in places such as airport terminals) **rather than smaller scale experiments** (e.g. AI-enabled detecting financial crime activities or credit scoring).

  Additionally, the **set-up of sandboxes** for the promotion of AI **is voluntary** in the current proposal and is left to the discretion of member states. For the benefit of creating a level-playing field, **the EBF suggests making this mandatory for all member states.** For the financial sector this would also require close collaboration with financial sector supervisors, which need to be well-equipped to support these activities.

Title VII: EU database for stand-alone High-Risk AI systems

Overall, EBF members would like to understand for which use cases/applications the EU database would be useful for. We also see risks in making it public and would therefore **suggest to make the database for Regulators only (see below comments on Art.60(3)).**

- **Article 60**: Additional details on how the registration process in the EU database will take place are needed. In case the registration process would take a long time, this could slow down the market entry for applications. Database registration should be simple, agile and should not delay the placement in the market of the service, not infringe any intellectual property rights and not disclose any confidential information.
- **Article 60 (3)**: As the public access to models (e.g., credit risk ones) may allow external subjects to modify some information distorting results in their favour, the EBF suggests the **database be available only to regulators.**

  Regarding the requirements in Annex VIII of the proposal, **the expected content and the intended purpose of including in the database the "electronic instructions for use" is not clear to members.** Would these instructions be intended for the users of this applications, or for the customers of the service? On one hand, according to Art. 13, high-risk AI systems shall be accompanied by instructions for use, so users would already have them. On the other hand, from the point of view of the client, who will not be a direct user of the system, the instructions would probably relate to – for example - the process of applying for a loan instead of how to use the AI model to calculate their credit scoring.

  The publication of 'Electronic instructions for use' **would also make the use of High-Risk models susceptible to manipulation, expose confidential information and may, as a result, reduce the incentive of firms to innovate and develop their own AI models**. An assessment of appropriateness is required in relation to disclosure of information, one which would allow firms to withhold disclosing this information publicly where there can be a reasonable expectation that security or confidentiality may be breached as a result of such disclosure.

Finally, another question raised by members relates to what has to be included in the EU database **in case that a high-risk AI system is just a component of a wider process or system.**

Title VIII: Post-market monitoring, information sharing, market surveillance

- **Article 62**: With regard to reporting of serious incidents and of malfunctioning, **the EBF highlights the fact that there are already several overlapping statutory incident and event reporting obligations for financial services both at the EU and the national level and it calls for harmonization for an alignment of reporting obligations arising from other EU legislation, such as the proposal for a Digital Operational Resilience Act (DORA)[8].** The regulatory process should involve mapping out all incident reporting obligations and evaluating the possibility to replace them with a central incident reporting Hub -ideally at Member State level- as suggested in the DORA proposal. At the moment, financial entities may be required to report a single incident multiple times to several authorities in different Member states and with each report to be filed in the local language and using dedicated national templates.

  This generates entirely unnecessary administrative costs, increases the risk of misunderstandings, and may even hinder the resolution of and recovery from the incident because valuable resources need to be diverted from the actual resolution of an incident to meeting the overlapping statutory reporting obligations. Furthermore, we would welcome a clarification on the **meaning of breach of obligations protecting fundamental rights.**

- **Article 64**: Introducing **direct and remote access** to the documentation and (training) data of providers, amongst others via API's **is disproportionate and goes far beyond the current mandate of supervisors, preceding any discussions on data driven supervision (and/or real-time supervision) and could even conflict with GDPR** (particularly regarding preventative audits). Processing of personal data should be proportional and this needs to be reflected in the proposal.

  Moreover, **a secure and standardized API Framework for this purpose does not currently exist** and the development of APIs or other technical means for remote access would likely require large investments and **would increase the attack surface for cyber-attacks** without bringing considerable benefits to market surveillance authorities that can always perform their duties on the providers/users' premises. **Therefore, we suggest amending Article 64 (1) to be in line with current supervisory practices.**

  In respect of **source code (Art. 64(2)),** the provision of this information to supervisors **could present a security risk.** To the extent that this code was exposed to a security breach, this presents a material risk both from a disclosure of proprietary information perspective but also from a vulnerability perspective should the code be used to potentially manipulate models. We therefore suggest that **access to source code is removed, or that a sufficiently high bar is included within the Act so that access is provided only in instances where there is a reasonable suspicion by a supervisor that a provider is in contravention of the Regulation.**

  In case of need related to monitoring, another option to consider is making documentation available on site, in order to reduce operational risks.

[8] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014,* 24 September 2020, COM (2020) 595 final

Title IX: Codes of Conduct

- **Article 69:** Developing codes of conduct should maintain **a perspective aimed at promoting the awareness around AI systems within the different stakeholders, representing a tool to enhance cultural development and accountability**. To support innovation, it is therefore important that codes of conduct **do not introduce barriers or friction to innovation processes and, ultimately, limit the scope of experimentation.**

  The requirements for high-risk AI systems are likely to be disruptive if applied to non-high-risk AI systems and impose disproportionate obligations. The adoption of such codes of conduct could lead to an excessive burden that could ultimately discourage the adoption of the AI system since it involves the voluntary alignment of non-high-risk systems with high-risk ones, in areas where there is almost no threat for fundamental rights. **We therefore suggest replacing the reference to "Title III, Chapter 2.2" in the first paragraph of Art. 69 with "proportionate and tailored requirements for non-high-risk AI systems, agreed on a voluntary basis".**

  Another approach could be leaving to stakeholders an open choice on how to pursue AI trustworthiness while adopting the codes for non-high-risk AI systems. We would also like to emphasize that alignment with global and industry—driven standards would be preferable to ensure consistency and meet industry best practices in EU and elsewhere.

  Overall, we feel that the goal of the proposal for businesses to voluntarily submit their AI solutions to the AI-regulation, will perhaps not have the desired effect. This is likely due to the binary distinction between high and low risk.

Title X: Confidentiality and Penalties

- **Article 71(3)**: The penalty set out in this provision for the violation of Article 10 on data sets is burdensome, especially when compared to the wording of the rule which, as seen above, appears to be very generic, open to different interpretations and very difficult to implement. We therefore recommend to **delete letter (b) of paragraph 3 from Article 71**, so that the violation of Article 10 will be addressed in Article 71 paragraph 4.

  Overall with regards to penalties, it is also necessary to take into account that these sanctions are cumulative with those provided by other texts, in particular GDPR.

Title XII: Final Provisions

- **Article 83**: According to this provision, the proposed regulation also applies to high-risk AI systems, that have been placed on the market or put into service *before* the date of application**, if those systems are subject to "significant changes" in their design or intended purpose**. It should be noted that **it is very costly to retrospectively comply with the requirements (e.g. regarding testing data) in a situation, where the AI system has already been developed, therefore it is necessary to clarify the definition of "significant".**
- **Article 85 (3b)**: It should be noted that Penalties (Article 71) should not be applied before the Regulation itself applies. Moreover, the EBF suggests deleting the following sentence "*Therefore the provisions on penalties should apply from (…)*" in Recital 88.

We also note the proposal for an amendment to Article 83 as described under Title I to clarify that the proposal shall apply to high-risk systems affected by the modification of Annexes I and III from 24 months following the entering into force of the delegated Acts defined in Articles 4 and 7.

ANNEX III

- **Paragraph 4**: On **high-risk AI systems used for employment, workers management and access to self-employment**, we note that with regards to promotion and termination decisions, it is important to clarify that **'making decisions' here is limited to AI systems that make explicit recommendations as to 'promotion and termination'.**

  The current drafting has the potential include other use cases that may have a connection to 'promotion and termination' **but are not used to make explicit recommendations or decisions.** For example, to the extent that an AI system was used 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.

  We note the purpose of the regime 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*'. As per the AI proposal, the EC notes that in the context of promotion and termination, use of AI should be high risk on the basis that it '*may appreciably impact future career prospects and livelihoods of these persons*.' On this basis, AI that is used in instances other than to make explicit recommendations relating to promotion and termination, **do not need to fall within scope**, as the AI system would not itself have an impact on future career prospects and livelihoods of these persons.

  Looking at the terminology of 'task allocation', given its vagueness, it could cover also "everyday issues", such as creating rosters and shifts for employees, which are not very relevant from the risk point of view. This could potentially cover a large amount of AI use cases, since the planning and directing daily work and allocating the work at the company and individual level are very important aspects of daily operations of the companies. We therefore suggest that in respect of 'task allocation', **this should be limited to instances where such task allocation will have an impact on 'future career prospects and livelihoods of these persons'.** For example, there may be instances where an AI system is used to allocate tasks based on capacity or specific skill sets of individuals, as opposed to evaluation of that individual from a performance perspective and would therefore not impact their career prospects or livelihood.

ENDS

For more information:

Liga Semane
Policy Adviser – Data & Innovation
l.semane@ebf.eu

About the EBF

The European Banking Federation is the voice of the European banking sector, bringing together 32 national banking associations in Europe that together represent a significant majority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that reliably handle more than 400 million payment transactions per day. Launched in 1960, the EBF is committed to a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu