13 June 2020

EBF_041600

EBF response to the European Commission AI White Paper Consultation - Annex

The European Banking Federation (EBF) welcomes the European Commission's White Paper on "Artificial Intelligence – A European Approach to Excellence and Trust" and the opportunity to provide comments to the proposals therein. This paper complements our response to the European Commission survey on the AI White Paper.

1. Ecosystem of Trust pillar

a) Avoiding duplication

AI provides significant opportunities in the European banking sector, ranging from enhancing customer experience, improving financial inclusion, cybersecurity, and consumer protection, to strengthening risk management and process efficiency. As a result, banks continue to invest in research and development of AI applications and the technology has come to play an integral role in a range of activities, including but not limited to: anti-money laundering, transaction monitoring, KYC, advanced/smart security events monitoring, fraud and anomaly detection, cyber threats, , customer service, and e-mail processing.

In order for European banks to continue to build on the potential of AI technologies, **the regulatory environment needs to be fit for the use of AI and enable innovation, while providing legal certainty** (e.g. on IP considerations), **and maintaining a strong level of consumer protection**. Similarly, **ensuring a level playing field across industries and geographies is of capital importance** to ensure the uptake of AI in the European banking sector and a high level of protection for individuals.

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

The White Paper recognizes that existing legislation, both sectoral and horizontal, continues to be applicable to the use of AI. **This recognition of existing regulation is crucial to ensure a level playing field and to avoid duplication**. In addition to being subject to the General Data Protection Regulation (GDPR) and to the Fundamental Rights of the EU, **the banking sector is subject to significant additional, specific regulation which ensures consumer protection, risk management, and financial stability in all services provided to customers, including those applications that could include the use of technologies such as AI.**

For example, banks are subject to prudential and conduct regulation, principles for effective risk data aggregation, operational and ICT risk management and to regulations imposing specific requirements on activities such as advice (Markets in Financial Instruments Directive II (MiFiD II)) or mortgage granting (Mortgage Credit Directive). If banks develop and introduce robo-advice applications to the market, for example, these would be considered as advice activities falling under the remit of MiFiD II. As such, the financial institution providing this service would be required to do a suitability assessment, in order to propose to consumers the products that can meet the clients' profile, considering the financial situation of the client, and comply with the relevant guidelines (e.g. ESMA Guidelines on certain aspects of the MiFid II suitability requirements).

With regards to risk, 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, 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.** In this regard, we would like to stress that the use of AI technology to assist or execute certain process does not necessarily introduce another category of risk.

b) Comments on the proposed approach

We are of the opinion **that new, AI specific legislation is not required and believe it is key to take into account the consequences that any rules could have for the competitiveness of European companies.** However, **guidance** developed by competent authorities on how to apply existing requirements to AI use cases could help firms to effectively apply their obligations under different regulatory regimes. This should be a collaborative process, with competent authorities working with each other, with input from industry and civil society. Any guidelines should not be overly prescriptive, as this would be in friction with the rapidly evolving nature of AI-related technologies. We also emphasize the importance of taking **a technology neutral approach**.

If the Commission proceeds with horizontal AI regulation, as proposed in the White Paper, we generally support the proposed approach to focus only on high risk AI applications. **An approach centred on prescriptive, wider regulation could hamper the adoption of this enabling technology and harm Europe's competitiveness globally**. Still, we express caution that there might be cases where regulatory arbitrage is possible, where

an activity can be performed by companies that fall outside a designated high-risk sector. In those sectors where activities can be performed subject to different regulatory regimes, the Commission should ensure that the exception foreseen in the White Paper (application regardless the sector) is applied to guarantee that high-risk applications are fully captured and that citizens safety and their fundamental rights are well protected.

Overall, in order to avoid uncertainty regarding the scope of this potential regulation, the Commission should develop clear and objective criteria for high-risk applications to ensure that only those applications that could cause serious harm to citizens (e.g. by putting their lives at risk) are captured.

We also share some concerns regarding the possible inclusion of "specific applications affecting consumer rights". The current formulation is very broad, creating again the risk of legal uncertainty as to the scope. Any "immaterial harms" to be addressed needs to be defined clearly. The Commission should ensure that only high-risk applications are captured, so that the proposed new requirements are consistently applied and without any differentiation per sector, country, or supervisor. This framework should not be extended to other activities or use cases with significantly lower risks.

We likewise stress once more the importance of taking a technology neutral approach. The focus on the applications of AI rather than on the technology itself is therefore welcome. Regulatory requirements should not apply to the underlying technology, but to which purpose it is put. Accordingly, any definition of AI used in potential legislation must be future-proof and avoid being overly broad in a way that could inadvertently include technologies that are not AI and do not pose the same risks. Any future definition should ensure it is focused on genuine AI and is future-proofed, for example by focusing on the technology's adaptive qualities. Using a definition such as the one proposed by the AI High-Level Expert Group (HLEG), risks that any system, including general automation processes which do not give rise to the primary issues identified in the White Paper, is subject to AI specific rules.

We welcome the opportunity to discuss in more detail, ahead of the issuance of potential legislation, a potential definition of AI that focuses on its key characteristics and is fit for regulatory purposes, i.e. easily understood, unambiguous and succinct.

Finally, in regard to the type of requirements proposed for high risk applications, we would like to note the impact some of them could have based on our experience of operating in a highly regulated sector. First, as the AI landscape continues to evolve, the way in which aspects of human oversight is integrated into AI systems will change. As such we caution against crystalizing an *exhaustive* list of human oversight examples into any legislative instrument. Second, we note that requirements for the provision of information disclosures to consumers need to be designed carefully to ensure that different groups, especially consumers, receive information that is relevant and understandable to them. Finally, in terms of governance we note that a strict ex-ante oversight could slow innovation and delay the launch of products/services leveraging AI to the market.

c) Voluntary labelling scheme for non-high risk AI applications

We have significant concerns with regards to the introduction of a voluntary labelling scheme and would not recommend establishing one. A "trustworthy" label for non-high risk applications implies that any application that does not carry the label is deemed "not trustworthy". By asserting this kind of social value, the label can no longer be considered truly voluntary. This runs counter to a risk-based framework as it would implicitly increase the requirements placed upon applications that are not high-risk, due to market discipline pressures. Furthermore, labels for data controllers can be complex:

- Labelling systems can be difficult to set up and **are likely to complicate and prolong the development and implementation of AI systems,** which are often scalable or self-learning building blocks, or encapsulated into larger systems in the form of internal or external components that are difficult to isolate, etc. AI is a fast evolving technology, but a label would be "static", assessing certain requirements at a particular moment in time.
- The **supply chain perspective** is important to consider. Would organisations as service consumers that are placed later on the chain have to inherit all the high risks resulted from service providers? This **points to the broader issue of AI technologies provided by external providers**, which could make meeting certain requirements of future labelling schemes difficult due to, for example, IP issues.
- We have concerns as to its **utility for consumers**, particularly on the ability to recognize whether, if a particular product or service does not have a label, the company did not apply for it or whether its absence means that the product/service does not comply with the requirements of the label scheme. This raises the issue of how to market and present the label to the consumer. Would it be when offering a particular service or through a different means, such as in the Terms & Conditions.
- A concern from some of our members is that it would not make sense to subscribe to a labelling scheme **that would only show that "trustworthy AI" is applied, regardless of the other technologies that may be in use.** The consumer needs to have access to trustworthy products or services as a whole, regardless of the technologies behind it. **There is a risk of consumer confusion about what having (or not having) a 'trustworthy AI' label really means**.

Regarding its design, if a voluntary labelling scheme is created, we would recommend that **the framework is more specific, simple, and follows a risk-based approach, taking into account the magnitude of the risks for the consumers of each particular application, and certifies specific applications, not the whole firm's activity.** Care would also be needed to ensure comprehensible and meaningful terminology, given this scheme would be cross-sectoral (for example, the meaning of stating that AI is sufficiently 'accurate'). Further clarification on how the scheme will be developed would also be helpful and we recommend the inclusion of a mechanism for consultation with industry on its creation.

To enhance trust in AI, we believe in **continuing investment in both scientific and academic research as well as education on the use of AI, its capabilities and the challenges involved.** Research into the actual and potential risks and ways to prevent

and mitigate them will help their identification in a timely manner. General or **consumer education** can help to eliminate potential myths and address doubts on its multiple applications and can prove to be more effective than a labelling scheme.

d) Governance

While not creating a new Agency is a positive step, the White Paper's proposal to create a new governance structure in the form of a framework for cooperation of national competent authorities may not fully address the risks of fragmentation of supervisory and or regulatory practices. **We therefore recommend that one of the explicit purposes of the network of regulatory authorities should be to encourage information sharing and cooperation on AI issues by different sectoral authorities**. This would be for the purposes of avoiding a situation where standards for similar activities are regulated more rigorously in some sectors than others, resulting in **'regulatory arbitrage'**. The network should also **encourage collaboration on AI issues by DPAs and sectoral authorities**, where an issue is relevant to the competence of multiple authorities so as to **ensure that any guidance and expectations are consistent and not in tension with each other.**

Finally, EU frameworks for experimentation should be encouraged so that authorities can **better understand the advantages of AI applications for companies and consumers, and how companies are mitigating potential risks to foster innovation**. These frameworks would facilitate the dialogue between authorities and companies, and would be help authorities to:

- Better understand technology and gain insight on how companies are using AI on specific applications, including in the financial sector.
- Promote the uptake of AI applications in various parts of the value chain.

To create a true Digital Single Market and facilitate a level playing field across member states, **such frameworks should be implemented at the European level.** The level playing field should also be respected in terms of different market players. It is important to make sure that these possibilities are not only open for the new market players but for all market players.

2. The Ecosystem of Excellence

a) Public-private cooperation

We welcome that the White Paper mentions the importance of cooperation with the private sector. Collaboration between the private and public sectors, including academia, in addition to helping set the research and innovation agenda, can help to tackle challenges with regards to AI and ensure resiliency to any future risks. For example, a member bank has an ongoing collaboration for scientific research purposes with a technology partner and a university to develop a use case to tackle ethical challenges of AI application in the banking sector.

b) Global view

The **global view on regulation should also be taken into account** and we welcome the European Commission's international cooperation efforts on AI mentioned in section 4H of the White Paper. However, we would like to flag restrictions of the use of technology developed outside the EU could risk putting EU firms at a disadvantage vis-à-vis other geographies. **We believe that any requirement should be applied on a 'service location basis', making sure that all services received by European citizens have similar requirements, regardless whether the model/ algorithm/ service/ product was developed in the EU or abroad**.

Finally, data is one of the key ingredients of Artificial Intelligence and machine learning and **initiatives to increase access to and sharing of data should complement actions to increase AI uptake across European industries**. Data pooling and sharing with the EU should be not just be enabled but also encouraged, in line with relevant data privacy and consumer protection rules.

3. Data requirements and AI

As data is a key element for the development of AI, we would like to share further observations in this regard.

We agree with the **Commission that the GDPR and Law Enforcement Directive already provide strong privacy and data protection regulation, which should not be duplicated**. The GDPR is a principle-based, technology neutral regulation that relies on a risk-based approach.

However, some members have flagged uncertainties and challenges regarding certain GDPR principles (e.g. data minimisation, storage limitation, purpose limitation, and user's right for an explanation) and obligations (e.g. restricted collection of sensitive data) in regard to AI development (including data processing for AI training purposes).

Some of these challenges **are also flagged by the European Commission's Expert Group on Regulatory Obstacles to Financial Innovation in their Final Report**[1] which notes that *"currently, firms may be held back due to uncertainties about how to comply with data protection rules when using AI and certain other technologies*". The text gives examples on how the interpretation of, for example, the data minimisation principle can pose questions when it comes to experimentation[2].

As a result, depending on the interpretation of GDPR principles and obligations by local and EU level supervisors (and the risk that it is too restrictive), companies may be limited when using AI to innovate, provide better services and safer solutions to consumers. **Legislators and supervisory authorities (SAs) should understand the interactions among the principles and obligations set in the GDPR and the needs of technology**

[1] Final report of the Expert Group on Regulatory Obstacles to Financial Innovation https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf

[2] Ibid.

developments, provide guidance (where needed) and assess compliance. Obstacles to the adoption of digital strategies and innovation should be removed.

We would also recommend conducting further research on reconciling purposes under the GDPR when it comes to AI application development and implementation, as this could help both supervisors and firms developing and implementing AI technologies and solutions.

Training data is considered a critical pre-requisite for any AI-application or implementation in order to be successful. Currently, the first step in most use cases is identifying the right amount of data and getting the relevant/suitable data. Common practices to address these challenges are the right selection of mitigating measures to be applied, such as data anonymisation and using synthetic data to reduce any risks whilst maintaining a certain level of quality in a data set. Different use cases therefore require different approaches to ensure desired model output. For example, in Know Your Customer (KYC) or fraud detection (where the AI system must able be to learn from meaningful data and determination of false-positives in order to accurately detect true anomalies) applying anonymisation to the training data could decrease the accuracy of the application.

Taking together the comments mentioned above, we would also like to share the following considerations regarding "training data" and "data and record keeping" requirements for high-risk applications:

- Having data sets that are sufficiently broad and representative can help to reduce bias and unintended outcomes. However, confirming with certainty that datasets are in fact sufficiently representative is challenging, and could require the collection of additional data, such as information on gender of individuals. Rather than a requirement to ensure that the system is trained on data sets that are sufficiently representative, which could be difficult to determine in practice without much greater collection of data subjects' personal data, a more suitable approach might be to require developers to determine whether there are any clear indications that the data is not representative, and then resolve accordingly.
- The fact that the volume of and diversity of data used is a direct contributing factor for the performance of AI applications makes exhaustive, long-term record keeping a challenge. Keeping all training data used for an AI application would be onerous and infringing to at least the principles of the GDPR. A prohibition on tracking certain sensitive data attributes (such as restrictions around special category data under GDPR) would also make a comprehensive assessment of the data representativeness more challenging.

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