POSITION PAPER

ESBG Position Paper on the European Commission consultation on the Artificial Intelligence Act

ESBG (European Savings and Retail Banking Group)

Rue Marie-Thérèse, 11 - B-1000 Brussels

ESBG Transparency Register ID 8765978796-80

July 2021

ESBG

I. General comments:

A.I. technology has only slowly began arriving on the market and as applications become more sophisticated, they will likely often become very unpredictable in their development. To ensure legal certainty, a level-playing field and no obstacles to innovation, a clear definition of artificial intelligence is needed. ESBG members very much welcome the proposed technology-neutral and future-proof definition of AI, and the Commission's risk-based approach to enable a proportionate regulation.

The Commission aims to turn Europe into the global hub for trustworthy Artificial Intelligence. If we of course share this idea on the principle, it should be recognised that this is a risky bet. Indeed, if European values are not ultimately adopted on an international scale, non-European solutions are potentially more efficient because they have been developed in less restrictive regulatory environments and could compete with European solutions.

II. Definition:

Artificial intelligence (A.I., or artificial intelligence, AI), machine learning (ML) and deep learning (DL) are three different things:

- Artificial intelligence is a science like mathematics or biology. It explores ways to build intelligent programs and machines that can solve problems creatively, which has always been considered a prerogative of humans.
- Machine Learning is a subset of artificial intelligence (AI), which gives systems the ability to learn automatically and improve from experience without being explicitly programmed. In ML there are different algorithms (e.g., neural networks) that help to solve problems.
- Deep Learning, or deep neural learning, is a subset of machine learning, which uses neural networks to analyse various factors with a structure similar to the human neural system.

These three differences need to be understood and used where appropriate in legal texts, to avoid creating regulatory uncertainty and to ensure risk-assessment methodologies factor in the type of A.I. (and A.I. learning) correctly. For example, Deep Learning is often hailed as the most likely ML approach to succeed in creating an AGI (Artificial General Intelligence), because its structure is similar to the human mind. However, certain potential issues with this method have already been identified:

- DL is limited when it comes to open-ended reasoning based on real-world common sense and knowledge, meaning that machines would not be able to distinguish between "Tom promised Mary to stop" and "Tom promised to stop Mary".
- Deep learning is self-sufficient and is made up of correlations, rather than abstractions. Problems that deal largely with common sense reasoning are mostly outside of what deep learning can cope with.
- Another problem often linked to deep learning is acquiring biases. If the training data set contains biases, the model will learn and consequently replicate those biases in its conclusions and predictions.

This is an example of how different types of technology can create different types of risks. Next, let us explore a definition of Artificial Intelligence application types more generally, which will make it easier for legislators to distinguish between A.I. types.

In the case of machine learning, which should primarily be covered by current regulation (if at all), a distinction is also made here between four different types of algorithms, which use different learning

methods for the methods: **supervised learning, unsupervised learning, semi-supervised learning, reinforced learning**. These algorithms determine the development possibilities and chances of the respective application as well as its limitations.

Using the term Artificial Intelligence to mix up these vastly different types of applications in everyday life (as well as in legal use) is not appropriate. It is further **essential to ensure that A.I. only legally refers to software that utilises machine-learning algorithms**, rather than being broad or vague in its definition. Too broad a definition leaves the door open to **misinterpretations and over-regulation of other existing computer systems, or even mathematical models**, that have been employed for a long time and have nothing to do with an A.I.. This is a matter of **level-playing field**, as these non-A.I. systems and practices cannot hope to compete with A.I. in the long run. Therefore, **over-regulating existing practices**, would essentially make the case for A.I. usage in every one of those cases, but **bar those incapable of building or affording A.I. from staying in the market.**

The definition of an AI system as provided in Article 3(1) in conjunction with the list of approaches and techniques in Annex I may be too broad, since it could potentially include more traditional software systems that should not fall under the scope of the proposal.

We believe that the definitions provided by the proposed Regulation (e.g. on AI systems) are different in some Member States to the definitions taken into account in the Guidelines issued by the national data protection authority. Also, there are other initiatives, such as the Council of Europe/CAHAI initiative of a **general framework for AI**, and the OECD framework for **classifying AI systems**, which should also be ensured to be aligned with the EU Regulation. In sum, we observe that each initiative is considering diverging definitions, which implies diverging scopes, and therefore, the regulatory landscape can create inconsistencies in the future.

III. Data-usage:

Introducing a general AI regulation for all applications inhibits the emergence of artificial intelligence in Europe. The EU is already limiting itself in how innovative it can be, due to excessive regulation that is often directed towards threats from large US-based technology firms but ends up hurting the innovation potential of EU-based companies, especially SMEs. **For the purpose of crime reduction (AML, CFT and AMLD6 Art. 2), AI requires data, and a potential review of current data sharing and data privacy regulation**. Otherwise, innovators will look to national legislators for increased flexibility, e.g., on the GDPR, which would end up defeating the purpose of such regulations, namely, to create a harmonised level-playing field across the EU.

With regards to Article 54 AI, without access to real data, A.I. development is fairly limited. So called "synthetic datasets" (fake or anonymised datasets to be used as templates to train A.I.) are insufficient and fairly limited in what they can teach A.I. Although synthetic datasets (i.e., generating new "artificial, noisy" data) would be useful for generating additional data when lacking a sufficiently large or unbalanced set of relevant data, it also has certain limitations such as perpetuating or even reinforcing bias by generating new (synthetic) data which is based on already biased data sets. This is even more the case when second order bias (e.g., ethnicity indication based on living area or income) is data imminent. Furthermore, information relevant for searching names or connecting data based on not standardised data (names for individuals or companies, addresses, phone numbers, etc.) via NLP (Natural Language Processing) is made impossible as encoding/decoding does not work via synthetisation. Adding "noise" as a countermeasure, i.e., randomly change certain attributes for synthetic data sets can also lead to further machine learning model performance deterioration and can only be applied when carefully and selectively applied.

In addition to data synthetisation, data anonymisation or pseudo-anonymisation can also be applied for machine learning. This is generally the case, but not applicable when respective names, addresses, telephone numbers etc. are regulatory requirements for respective screening and connecting customer and transaction data for KYC, sanctions and embargoes and respective predicate offense purposes. Here, NLP (natural language processing) for e.g., named entity resolution algorithms cannot (sufficiently) work with (pseudo-)anonymised data.

IV. Developer protection:

European AI developers and users must be sufficiently protected internationally. As AI do not discriminate against physical locations, and many different countries across the world have different interpretations of copyright and liability when it comes to AI applications. This consideration is currently missing from the draft regulation.

On one side, we consider that the scope of the obligation to register high-risk AI systems should be limited further than in the EC proposal, to avoid impacts to **intellectual property**, and to avoid possible duplicity of tasks and obligations between the AI Regulation and other regulatory frameworks (e.g. prudential – internal model reviews). On another side, even though some of the obligations placed on providers or users of high-risk AI systems are expected to be considered as fulfilled by compliance of the CRD framework, we would also raise concerns on the possible duplicity of tasks, again, and on the consistency of both sets of regulatory frameworks.

V. Proportionality and level-playing field

Furthermore, there is a **risk of unintentional over-regulation of weak AI**, e.g. because of **unaffordable penalties for any unintentional mistakes** A.I. developers might make, which are likely to prevent individual developers, as well as SMEs and even larger companies in Europe (and our MENA partners) from developing their own AI applications and leaving the digital market to other countries. At the same time, we appreciate the Commission's bold and strong stance on illegal types of A.I., which would undoubtedly lead to great societal harm. However, we do not quite understand why public entities and private entities are viewed differently in this scope, or why military applications – the most dangerous of all – are completely exempted from the regulation. We hope that this is a strategic move that will allow separate and more stringent regulation of such dangerous A.I. and would appreciate some form of **acknowledgement of this via a recital.**

As for the private-public distinction, **many private companies are carrying out work for the public sector** and rarely does the public sector operate its own public solutions, especially in the software space. Therefore, we wish to **clarify how this regulation will affect private actors, who are working for the public good**, in particular we are concerned about our own **efforts to mitigate financial crime, which is heavily dependent on the usage of A.I.** systems. As such, we propose that **the fight against financial crime be exempted from the scope** of this regulation. An alternative approach could be some form of supervisory approval for this kind of usage, that would replace the self-assessment in such cases. When it comes to **KYC, AML/CFT and fraud**, any and all additional bureaucracy and limitation plays into the hands of criminals.

VI. Supervisory Authorities:

Similar to other initiatives, in this case too we consider that the rules on the enforcement of the Regulation are not clear enough, and do not anticipate enough resources for the supervision that can ensure compliance with the Regulation.

ESBG members appreciate the recognition that the **Union legislation on financial services already includes internal governance and risk management rules and requirements** which are applicable to regulated financial institutions in the course of provision of those services, including when they make use of AI systems.

We support the decision to ensure coherent application and enforcement of the obligations under the AI Regulation and relevant rules and requirements of the Union financial services legislation. These **designate the authorities responsible for the supervision and enforcement of financial services legislation**, including where applicable the European Central Bank, as competent authorities for the purpose of supervising the implementation of this Regulation on topics such as market surveillance activities and AI systems provided or used by regulated and supervised financial institutions.

To integrate the **conformity assessment procedure** and some of the providers' **procedural obligations in relation to risk management**, post marketing monitoring and documentation into the existing obligations and procedures under Directive 2013/36/EU.

However, we would appreciate some more clarity from EU institutions regarding the compatibility of data protection supervisory powers and powers on enforcement of the AI Regulation.

On the planned action on AI in the Digital Finance Strategy, the Commission has planned to invite the ESAs and the ECB to explore the possibility of developing regulatory and supervisory guidance on the use of AI applications in finance. We wonder if this action is still needed as the regulation proposal on AI designates the authorities responsible for the supervision and enforcement of the financial services legislation as competent authorities for the purpose of supervising the implementation of the AI regulation. Processes and methods are already known and in place.

VII. Code of Conduct:

The Commission wishes to encourage providers of non-high-risk AI systems to create codes of conduct intended to foster the voluntary application of the mandatory requirements applicable to high-risk AI systems but also to apply additional requirements on a voluntary basis.

ESBG members agree on the principle and convene that it could generate a virtuous behavior on the market. Nevertheless, this may lead to a multiplication of different voluntary codes with very different levels of commitments, which may **ultimately lead to confusion on the part of users and consumers.** Moreover, **those codes of conducts could represent a new regulatory layer that could hinder innovation** and, at the end, **going against the original goal of the Commission to be proportionate in the approach.**

VIII. Biometric identification of natural persons:

We have understood that under the new rules, all AI systems intended to be used for remote biometric identification of persons will be considered high-risk and subject to an-ex ante third party conformity assessment including documentation and human oversight requirements by design. Will the financial services firm and their providers, who rely on biometric identification to onboard customers remotely

and comply with know-you-customer (KYC) requirements, will also be in scope of the full set of requirements in the AI regulation?

IX. Conclusion:

We support the Commission in its efforts to create a clear legal framework for artificial intelligence which does not inhibit innovation and at the same time provides security for all market participants. We are particularly pleased with the Commission's philosophical approach to promoting "digitalisation with a human face". We believe that trustworthy AI in cooperation with human expertise will be of great value to European society. We particularly emphasise the interaction between man and machine. We firmly believe that both humans and machines are irreplaceable. However, we must ensure that new regulation does not inadvertently cripple our markets, dampen innovation and opportunities.

About ESBG (European Savings and Retail Banking Group)

ESBG represents the locally focused European banking sector, helping savings and retail banks in 21 European countries strengthen their unique approach that focuses on providing service to local communities and boosting SMEs. An advocate for a proportionate approach to banking rules, ESBG unites at EU level some 900 banks, which together employ more than 650,000 people driven to innovate at roughly 50,000 outlets. ESBG members have total assets of €5.3 trillion, provide €1 trillion in corporate loans (including to SMEs), and serve 150 million Europeans seeking retail banking services. ESBG members are committed to further unleash the promise of sustainable, responsible 21st century banking. Our transparency ID is 8765978796-80.

European Savings and Retail Banking Group – aisbl
Rue Marie-Thérèse, 11 ▪ B-1000 Brussels ▪ Tel: +32 2 211 11 11 ▪ Fax : +32 2 211 11 99
Info@wsbi-esbg.org ▪ www.wsbi-esbg.org

Published by ESBG. July 2021.