Brussels, 23 July 2021
CDO

Position paper on a proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act)

The **European Association of Co-operative Banks** (EACB) represents, promotes and defends the common interests of its 27 member institutions and of cooperative banks, with regard to banking as well as to co-operative legislation. Founded in 1970, today the EACB is a leading professional lobbying association in the European banking industry. Co-operative banks play a major role in the financial and economic system. They contribute widely to stability thanks to their anti-cyclical behaviour, they are driver of local and social growth with 2.800 locally operating banks and 51,500 outlets, they serve 209 million customers, mainly consumers, SMEs and communities. Europe's co-operative banks represent 84 million members and 713,000 employees and have an average market share in Europe of about 20%.

For further details, please visit www.eacb.coop

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Fax (+32 2) 230 06 49 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail : secretariat@eacb.coop

Introduction

The European Association of Co-operative Banks (EACB) is happy to contribute to the discussion on the Artificial Intelligence (AI) legislative proposal.

The EACB recognises that the AI proposal is the Commission's first ever legal framework on the matter, which addresses the risks of AI and aims to position Europe to play a leading role globally. It should be recognised that this is a risky bet. If European values were not ultimately adopted on an international scale, European companies would be at a disadvantage compared to non-European players active in less restrictive regulatory environments.

We believe that the European Commission, the European Parliament and the Council should remain vigilant to ensure that European players are not unduly constrained in their prospect of developing innovative AI solutions compared to international competitors.

We would like to highlight the following points:

- The EACB welcomes the Commission's risk-based approach as basis for a proportionate legal text. The Commission suggests a risk-pyramid approach: the higher the risk (for users) using AI system, the more additional measures.

- We appreciate the technology-neutral and future-proof definition of AI, recognising that AI is a "fast evolving family of technologies" that is constantly developing. Nevertheless, combining the definition of artificial intelligence system together with the techniques and approaches of Annex I of the proposal, we observe that the scope of the Regulation is becoming quite wide as it also includes rule-based approaches.

- We believe it is of paramount importance to make sure that the AI proposal will not add new and burdensome requirements for the banking sector and create conflicts and overlaps with existing rules: e.g., sector-specific regulation (CRD, CRR).

- We particularly value the Commission's human-centric perspective in designing AI rules:
  - The responsibility for an action or a decision still lies with a human being;
  - Actions and decisions of an AI system have to be traceable and understandable by humans using it; and
  - Actions and decisions of an AI system can always be changed/corrected by a human being (human oversight).

- We understand that the Regulation's intention is to protect the safety and fundamental rights of EU citizens, thus that the requirements for high-risk AI systems are only targeted at AI applications that could possibly pose risks to natural persons.

- Generally, some provisions of the Regulation contain somewhat vague wording, e.g., the definitions provided for "remote biometric identification system" and "user". Moreover, we believe that the definition of 'developer' and 'end user' are missing from the legal text. These points should be further clarified in order to guarantee legal certainty for providers, developers and users of AI systems.

- Regulatory sandboxes are useful for the development of AI. However, their objectives and entry criteria should be clear and made public in order to ensure a high degree of transparency and a level playing field in the entry process.

- According to the Digital Finance Strategy[1], the Commission has planned to invite the European Supervisory Authorities (ESAs) and the European Central Bank (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 AI proposal designates the authorities responsible for the supervision and enforcement of financial services legislation as competent authorities for the purpose of supervising implementation. Processes and methods are already known and in place.

- We wonder how AI systems can be prevented from being biased. This requirement is not realistic as it cannot be guaranteed that datasets will be fully correct or complete. We believe that errors should be minimised and that the training, validation and testing of the AI system should be as complete as possible. To ensure a fair treatment an ex-post revision should be made possible.

- Finally, we wonder who decides what data is of good quality. An external institution cannot decide this because it doesn't understand the use of the AI system as much as the company that develops it. And if the company makes this decision, a conflict of interests comes into play.

EACB's specific comments

➢ AI and CRD frameworks

The EACB is pleased to see recognised in Recital 80 that EU 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.

Ensuring coherent application and enforcement of the obligations under the new AI Regulation and relevant rules and requirements of the Union financial services legislation is of paramount importance.

Recital 80 states that authorities responsible for the supervision and enforcement of financial services legislation should be designated as competent of supervising the implementation of the AI act. It also mentions that in order "*to further enhance the consistency between the proposed AI Regulation and the rules applicable to credit institutions regulated under Directive 2013/36/EU (CRD), it is appropriate 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 the CRD. In order to avoid*

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU, COM/2020/591 final.

overlaps, limited derogations should also be envisaged in relation to the quality management system of providers and the monitoring obligation placed on users of high-risk AI systems to the extent that these apply to credit institutions regulated by the CRD".

The content of Recital 80 is reflected throughout the following articles of the AI proposal:

- Art. 9 on risk management procedures; Art. 17 on quality management system; Art. 18 on the obligation to draw up technical documentation; Art. 20 on automatically generated logs; Art. 29 on obligations of users of high-risk AI systems. All referring to Art. 74 of the CRD on "Internal governance and recovery and resolution plans".
- Articles 19, 43 on ex-ante conformity assessment, and Articles 61 and 63 on post-market monitoring and market surveillance authorities, which refer to Articles 97 to 101 of the CRD.

➔ **While we appreciate the reference throughout the AI proposal to existing CRD provisions applicable to credit institutions in order to prevent overlapping requirements by the different regulations, we believe that further clarity is needed as regards the interactions of the two frameworks** (e.g., regarding the ex-ante conformity assessments foreseen as part of the Supervisory Review and Evaluation Process (SREP)).

We also note that the proposed Regulation lacks respective references to CRR provisions applicable to credit institutions using rating systems in the context of creditworthiness assessments and credit scoring.

➢ **CRR provisions on creditworthiness assessments and credit scoring**

According to the currently proposed classification of high-risk AI systems, AI systems used to evaluate the creditworthiness of natural persons and to establish their credit score, would fall under the remit of this Regulation and would need to fulfil the requirements set out for high-risk AI systems. As regards the use of such AI systems by credit institutions regulated under Regulation 575/2013 (CRR)[2], we see significant overlaps and even conflicting provisions between these two frameworks.

The CRR already foresees comprehensive requirements for the implementation of rating systems, including on the integrity of the assignment process (Art. 173), the use of models (Art. 174), the documentation of the rating system (Art. 175) and data maintenance (Art. 176), as well as on governance aspects (Art. 189). The proposed rules under the AI Regulation do not consider these existing requirements and would therefore create significant overlaps.

Additionally, internal models used by credit institutions already need to be approved by the competent authorities. This would overlap with the newly introduced requirement of obtaining an ex-ante conformity assessment for AI systems used as part of the creditworthiness assessment or credit scoring foreseen under the SREP.

[2] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012.

➔ **We believe that overlapping or conflicting regulation needs to be avoided and sector-specific legislation such as the CRR should prevail. Where the prudential framework already outlines requirements for banks' AI risk systems/applications those are the ones that should apply.**

➢ **Conformity assessment, Art. 19 (2) and Art. 43 (2)**

As pointed out in our comment above, the EACB believes that the use of AI systems for creditworthiness assessments and credit scoring by credit institutions is already sufficiently regulated by the provisions in the CRR and an additional ex-ante conformity assessment as part of the SREP would overlap with the provisions of the CRR.

➔ Notwithstanding the above, **if an additional ex-ante conformity assessment for high-risk AI systems referred to in point 5(b) of Annex III were to be integrated into the SREP as referred to in Art. 97 to 101 of the CRD, we believe that further guidance concerning the procedure foreseen for the assessment and the expected interaction between credit institutions and the competent authorities is necessary**.

➢ **Definitions**

- **'Artificial intelligence system' (AI system), Art. 3(1) and Annex I**

  Co-operative banks have been exploring the possibility offered by AI systems with the GDPR in mind. When we look at the proposal, there are a couple of elements relevant to us, in particular in the area of credit scoring and creditworthiness assessment. Banks are one of the earlier adopters of AI systems.

  Combining the definition of artificial intelligence system (Art. 3(1)) with the techniques and approaches of Annex I, we observe that the scope of the Regulation appears to expand as it also includes rule-based approaches.

  The current definition and scope provided by the proposed Regulation would include any logic and knowledge-based approaches. The mere use of such techniques and approaches clearly lack the characteristic of displaying "intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals" that the Commission used in its 2018 Communication on "Artificial Intelligence for Europe" to define AI systems[3]. We strongly believe that such systems (as set out under Annex I (b)) should only be considered as AI if they are able to automatically adapt without human intervention, or in other words, if such rule-based techniques have a self-learning character. Therefore, we propose a clarification to Art. 3 (1) where only rule-based approaches (Annex I (b)) without human intervention possibilities are in scope of the AI system definition. Without such a

[3] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, COM(2018) 237 final.

clarification on the proposed broad scope, the Regulation would create an unnecessary burden and high administrative efforts for many providers and users of such established software systems. Furthermore, we feel that 'decision' is clearer and more reflective of market practice than 'outputs'. Finally, we agree with the combination of Art. 3 (1) and the techniques and approaches as set out in Annex I (a) & (c) as a definition of an AI system.

➔ **We would welcome a more targeted approach, limited to rule-based techniques and approaches built on AI in the sense that such systems without human intervention should fall within the scope of an AI system.**

- **'Provider', Art. 3(2)**

We believe that the definition of 'provider' is not clear because it means the legal entity that develops AI systems but also has AI systems developed. This is not applicable for a lot of banks that have outsourced their IT to a different legal entity. It is necessary to define the roles of the legal entity that develop AI systems, e. g. an IT service provider, and the legal entity that has an AI system developed, e. g. a financial institution, and the role of the end user or the consumer, e. g. the client of the financial institution that interacts with the AI system, e. g. a chatbot. The process of defining a legal entity as either developer or user should be based on an individual AI system and can vary between AI systems, since a financial institution can use the AI system of an IT provider and would therefore be the user, or develop an AI system and in this case would be a developer. We would like to emphasize that entities are still struggling with role appointments under the GDPR (processor vs. controller) and hope to avoid this discussions and role ambiguity in proposed future legislation.

➔ **For the above reasons, we suggest replacing the definition of 'provider' with 'developer'.**

- **Need to better define the different actors in the chain: 'User', 'end user, 'operator'**

Because of the main reason given on the unclear definition of provider, we believe **it is necessary to better define the different actors in the chain involved in the AI system by amending the definition of 'user' and by adding the definition of 'end user'**. The suggested definition of 'user' in the Regulation does not clearly state if the user is a company (e.g., a bank) that uses an AI system that was developed by a different company (IT developer), or the end user (e.g., the customer of a bank).
Within the financial sector we face two different situations: firstly, the customer who is faced with the decision of a client-facing AI model (e.g., in case of automated decision by the co-operative bank on a credit card request by the customer); secondly, the employee who gives follow-up to the decision of an AI system in detecting fraudulent transactions (e.g., in case of a mortgage-loan request by a customer), which is a non-client-facing AI system.

Finally and in the same spirit of clarification, **we suggest deleting the definition of 'operator'** as it suggests too many different players can be an operator.

- **'Testing data', Art. 3(31)**

  We believe that biases and errors will not be identified when the validation data has the same characteristics as the data that was used for the training of the AI system.

  ➔ **Therefore we suggest making it clear in Art. 3(31) that the testing dataset must be a separate dataset.**

- **'Remote biometric identification system', Art. 3(36)**

  We understand 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. It is not clear to us whether financial services firms 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.

  On another note, Art. 3(36) provides the following definition for a remote biometric identification (RBI) system: *"[…] an AI system for the purpose of identifying natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified".*

  The wording in the second part of the definition would lead to the conclusion that, in case the user of the AI system knows that the person is present and can be identified, the AI system would not classify as an RBI system and would hence not fall under the classification as a high-risk AI system.

  ➔ **We believe that considering the above observations, further clarifications or a more precise definition are needed to avoid legal uncertainty and diverging interpretations by the competent authorities within the Union.**

- **'Regulatory sandbox', Art. 3(45)new**

  We note that while the AI proposal dedicates specific articles on AI regulatory sandboxes (Articles 53 – 55), a definition of regulatory sandbox is missing from the text.

  ➔ **We would appreaciate having a definition of regulatory sandbox in the proposal.**

➢ **<u>High-Risk AI Systems: classification rules for high-risk AI systems</u>**

In line with the general intention of the Regulation to protect the safety and fundamental rights of EU citizens, the high-risk AI systems listed in Annex III as referred to in Art. 6(2) focus on the intended use of these AI systems that could possibly harm natural persons. **This limitation should also be reflected in the respective article of the Regulation**.

- **Unrealistic requirements of training, validation and testing data sets, Art. 10 (3)**

According to the first sentence of Art. 10 (3), training, validation and testing data sets shall be relevant, representative, free of errors and complete. This requirement is absolutely not realistic as it cannot be guaranteed that datasets will be fully correct or complete.

➔ **Therefore, we suggest rephrasing Art. 10 (3) to the effect that errors should be minimised and that training, validation and testing should be as complete as possible.**

- **Transition period for delegated acts amending Annex III, Art. 7(1) and Art. 73**

According to Art. 7, the Commission can update the high-risk list in Annex III with delegated acts in accordance with Article 73. However, the proposed text of the Regulation does not foresee any transition period for AI systems newly added to Annex III via respective amendments by the Commission. However, we understand from an exchange with the Commission that the requirements for newly defined high-risk AI systems shall be applicable only two years after the delegated act enters into force allowing for a sufficient transition period.

➔ **Therefore, we suggest adding the transition period of at least two years to Art. 73.**

- **Exemption for small-scale providers**

Recital 37 states that "*Considering the very limited scale of the impact and the available alternatives on the market, it is appropriate to exempt AI systems for the purpose of creditworthiness assessment and credit scoring when put into service by small-scale providers for their own use."* The same concept is also reported on Annex III point 5(b).

We would prefer a more precise expression than "it is appropriate". It has to be clear if small-scale providers are exempt or not.

➔ **We find the expression "appropriate" to be unclear and therefore suggest clearly stating whether small-scale providers are exempt or not. Furthermore, if they are exempt, it should be reflected throughout the Regulation.**

- **Sandboxes**

While we understand that regulatory sandboxes are useful for the development of AI, we think that the language used in the AI proposal is too vague. A definition of sandbox or a reference to a definition is not provided in the AI proposal. According to the definition[4] provided by the EBA,

[4] EBA Report on "FinTech: Regulatory sandboxes and innovation hubs". The definition used by the EBA of Regulatroy sandboxes is the following: "Regulatory sandboxes: these provide a scheme to enable firms to test, pursuant to a specific

sandboxes may also imply the use of legally provided discretions by the relevant supervisor. Furthermore, the Regulation does not give any hint on what will be the selection criteria that determine how companies are selected, or the goals that are pursued with the regulatory sandboxes, e. g. are they meant to foster the development of AI systems for new use cases? If so, how are these use cases selected?

Furthermore, we want to avoid market distortions by giving an advantage only to a few selected companies. It seems that sandboxes are designed exclusively to offer advantages to a few selected companies, while other enterprises have to develop their AI systems without the support and the improved environment. We are of the opinion that regulatory sandboxes should only be allowed if all companies have access to them. We believe that sandboxes should be open to both new (start-up) and incumbent (e.g., banks) FinTech (intended as technology-enabled innovation, as per the definition adopted by the Commission) providers. To prevent disadvantages to the companies without access, it should be possible for companies to establish their own regulatory sandboxes separate from their existing IT operations. A level playing field has to be guaranteed with those outside the sandbox, thus transparency on the experiments going on and any regulatory 'lenience' have to be transparent in order to avoid market distortions. The information in the reports that Member State competent authorities submit to the European AI Board and the Commission (Art. 53.5) should be made available to the public, so all companies can learn from the activities taking place in the sandbox.

Moreover, and as a general observation by reading Art. 53, there is a dichotomy between the willingness to set up regulatory sandboxes within the EU to foster AI innovation and the fact that the relevant participants in the sandbox should comply with "strict regulatory oversight" (Recital 71) of the legislative proposal on AI and, where relevant, other Union and Member States legislation supervised within the sandbox (Recital 72).

- ➔ **We suggest clearly spelling out in Recital 72 and/or Art. 53 that the objectives of the regulatory sandboxes and the entry criteria should be clear and made public in order to ensure a high degree of transparency in the entry process. Furthermore, we suggest that the lessons learnt in the sandboxes are made publicly available so that companies without access can benefit as well.**

- **<u>Codes of conduct, Art. 69</u>**

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.

We note that this may lead to a multiplication of different voluntary codes, 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, go against the original goal of the Commission to be proportionate in the approach.

testing plan agreed and monitored by a dedicated function of the competent authority, innovative financial products, financial services or business models. Sandboxes may also imply the use of legally provided discretions by the relevant supervisor (with use depending on the relevant applicable EU and national law)4 but sandboxes do not entail the disapplication of regulatory requirements that must be applied as a result of EU law." Page 5.

Contact:

The EACB trusts that its comments will be taken into account.

For further information or questions on this paper, please contact:

- Ms Marieke van Berkel, Head of Department Retail Banking, Payments, Financial Markets (marieke.vanberkel@eacb.coop)
- Ms Chiara Dell'Oro, Senior Adviser for Digital Policies (chiara.delloro@eacb.coop)