Input from the European Savings and Retail Banking Group (ESBG) on the technical negotiations on the Artificial Intelligence Act

Definition and scope

ESBG members argued for a narrow scope, since a scope that is too broad could potentially include more traditional software systems that should not fall under the scope of the proposal.

- The definition is open, undefined and too extensive. It includes any massive data processing technique, even the more traditional and simply programming. Rules should only be established for complex AI systems capable to learn.

- Additionally, the AIA, as an horizonal initiative, establishes rules on AI systems that are already regulated by sectorial rules (financial and insurance sectors).

Overlap with other pieces of legislation

When it comes to data protection, the GDPR regulates the processing of personal data, also when it is done by AI systems. The GDPR establishes a regime (principles, liabilities, and governance) for algorithms created by personal data or added to a personal data processing.

- Chapter II GDPR. General principles: legality, loyalty and transparency, limitation of the purpose, minimization of data, accuracy, limitation of the term of conservation, integrity and privacy.

- Article 24 GDPR. *Responsibility of the controller*
  1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. […]

- Article 25 GDPR. *Data protection by design and by default:*
  1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards

into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. […].

- Article 30 GDPR. *Records of processing activities*.

- Article 32 GDPR. *Security of processing:*
  1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate […].

- Article 35 GDPR. *Data protection impact assessment:*
  1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. […].

Article 5 – Facial recognition

When facing AML/FT obligations, obligations imposed to essential services operators and personal data protection requirements, financial entities have to deal with issues derived from identity theft. The main scenarios of identity theft are those related to the registration of customers with a false identity, the fraudulent use of credit or debit cards by people who are not the legitimate owners, and the fraudulent use of credit or debit cards in commercial establishments, in online purchases or at ATMs.

The identity verification for onboarding processes and performing operations remotely arises different issues. A diligent actuation by the financial entities, in accordance with the procedures established by the relevant authorities to verify the identity of people, is not enough to guarantee an adequate and reliable method taking into account the current state of science. For that reason, the use of biometric data to verify the identity of customers is a matter of public interest, even if it is previously authorized by the user.

The prohibition of AI systems for facial recognition would limit the possibilities of financial institutions to offer services remotely and therefore would hamper innovation in the sector.

In addition, as rightly underlined by the Council in its final compromise text (recital 8), it is important to distinguish the uses of biometric authentication systems. Please find below an extract from recital 8:

“Such a definition excludes verification/authentication systems whose sole purpose would be to confirm that a specific natural person is the person he or she claims to be, as well as systems that are used to confirm the identity of a natural person for the sole purpose of having access to a service, a device or premises. This exclusion is justified by the fact that such systems are likely to have a minor impact on fundamental rights of natural persons compared to remote biometric identification systems which may be used for the processing of the biometric data of a large number of persons.”

In our view, it is very important to be clear in the regulation on the definition of AI systems intended to be used for remote biometric identification. We would indeed recommend to base on the Council argumentation the recommendation to exclude from the scope of the regulation verification/authentication systems used by banks to onboard or identify customers remotely.

Article 47: Derogation from conformity assessment procedure
We have no comments on this matter.

Article 54: Further processing of personal data for developing certain AI systems in the public interest in the AI regulatory sandbox
To react on this matter we need to understand why MEP Vos wants to delete this article. What is the purpose?

About ESBG (European Savings and Retail Banking Group)

ESBG is an association that represents the locally focused European banking sector, helping savings and retail banks in 17 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 885 banks, which together employ 656,000 people driven to innovate at 48,900 outlets. ESBG members have total assets of €5.3 trillion, provide €1 trillion billion in corporate loans, including SMEs, and serve 163 million Europeans seeking retail banking services. ESBG members commit to further unleash the promise of sustainable, responsible 21st century banking. Learn more at www.wsbi-esbg.org.

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