BETTER FINANCE
The European Federation of Investors and Financial Services Users
Fédération Européenne des Épargnants et Usagers des Services Financiers

BETTER FINANCE responds to EIOPA's Public Consultation on the Opinion on AI Governance and Risk Management

Author

Sébastien Commain | Senior Research & Policy Officer

About BETTER FINANCE

BETTER FINANCE — the European Federation of Investors and Financial Services Users — is the voice of European citizens as savers, investors, and financial users at the EU level. Working independently from the industry, BETTER FINANCE serves as an independent hub of financial expertise for the direct benefit of individual shareholders, investors, savers, life insurance policyholders, pension fund participants, and mortgage borrowers across Europe. Their work aims to promote research, information, and training on investments, savings, and personal finances to lawmakers and the public. BETTER FINANCE counts 40 independent, national, and international member organisations, sharing similar objectives from the EU Member States as well as Iceland, Norway, Turkey, Lebanon, and Cameroon.

Executive Summary

BETTER FINANCE welcomes EIOPA's draft Opinion on AI governance and risk management in insurance undertakings. As the European-level representative of life insurance policyholders, BETTER FINANCE fully support EIOPA's risk-based approach to the use of AI systems and its call for appropriate safeguards.

It is the view of BETTER FINANCE that all AI systems in insurance need to be subject to a proper risk assessment, and that where threats to customers' interests are identified, safeguards proportionate to these risks must be put in place, including a sound data governance, effective human oversight, transparent information of customers and effective redress mechanisms. Only then can the deployment of AI in insurance be expected to improve the welfare of policyholders.

Rue d'Arenberg 44, 1000 Bruxelles
02 514 37 77
www.betterfinance.eu

Questions and Answers

Context, objective and scope

Q1: Do you have any comments on the context and objectives of the Opinion?

BETTER FINANCE supports the stated objective of the Opinion to "provide guidance on how different provisions of insurance sectorial legislation should be interpreted in the context of AI systems".

We concur with EIOPA's view that the Opinion should not set out new requirements beyond those established by the Level 1 legislation. Nevertheless, we do believe that providing further clarity regarding supervisors' expectation from firms implementing these Level 1 requirements is essential to ensure that policyholders are adequately protected against the risks that the deployment of AI systems in insurance undertakings may pose.

Q2 - Do you have any comments on the scope of the Opinion?

We support the proposed scope as regards types of AI systems to be covered by the Opinion. Avoiding duplication of requirements is essential for a competitive insurance industry; ensuring that transversal —the AI act— and insurance sectoral legislation together provide a comprehensive framework that leaves no AI system unregulated is equally essential to enable customers to trust insurance undertakings in using these systems responsibly. It is, therefore, crucial that the Opinion clearly states that any AI system deployed by an insurance undertaking that is not covered by the requirements of the AI Act (and derived legislation) falls under the scope of this Opinion and should be subject to appropriate requirements under insurance sectoral legislation.

AI governance and risk management framework

Risk-based approach and proportionality

Q3 - Do you have any comments on the risk-based approach and proportionality section? What other measures should be considered to ensure a risk-based approach and proportionality regarding the use of AI systems?

We support the risk-based and proportionality approach set out in the Opinion. We stress the importance of setting appropriate supervisor expectations for all non-high risk AI systems used by insurance undertakings. A proportionate approach to these expectations must acknowledge the variety and varying levels of risk that these systems entail for insurance undertakings' customers. Seemingly trivial uses of AI in internal processes may end-up disrupting services to customers: insurance undertakings should be expected to conduct (and document) a proper assessment before considering that an AI systems is "low risk".

Risk-management system

Q4 - Do you have any comments on the risk management system section? What other measures should be considered regarding the risk management system of AI systems?

We generally support the supervisory expectations laid down by the proposed Opinion regarding the risk management system. We fully share EIOPA's view that "[t]he responsible use of AI systems is not achieved by a standalone measure, but by a combination of different risk management measures". The six areas of risk management listed in section 3.7 —fairness and ethics, data governance, documentation and record keeping, transparency and explainability, human oversight, accuracy, robustness and cybersecurity— are all, in this sense, equally important.

We nevertheless note that the Opinion does not list of section 3.7 the environmental impact of AI systems amongst the items that the risk management systems should consider: the deployment of AI-systems may significantly increase the energy consumption of an undertaking, which may induce a reputational risk that the firm should assess under Art. 46.2 of the Solvency II Directive.

We welcome EIOPA's note that "the approach to AI systems should also include accountability frameworks, regardless of whether the AI system is developed in-house or in collaboration with third parties". Indeed, the distinction between developers and deployers of AI systems may be relevant for regulatory and operational purposes, but is totally irrelevant from the standpoint of (prospective) customers using an AI-based service.

The insurance undertaking must remain liable towards the customer for any damages caused by the undertaking's use of AI systems, regardless of whether the undertaking is the developer of the system or merely the deployer of a solution provided by a third party, a liability that derives from Article 49 of the Solvency II Directive. It would be unacceptable that insurance companies could eschew their responsibility towards their clients by outsourcing the development of AI systems.

We also support EIOPA's call, in section 3.10, for the "roles and responsibilities of different staff [to be] clearly defined", and the adequate training programmes provided to the relevant staff. Employees will constitute the "front line" of risk management: it is essential that staff members who use AI systems on a daily basis have the appropriate training to identify risks of misuse, unethical outcomes and potential biases, inaccuracies and data security breaches.

Fairness and ethics

Q5 - Do you have any comments on the fairness and ethics section? What other measures should be considered to ensure a fair and ethical use of AI systems?

We appreciate the reminder that "insurance distributors shall always act honestly, fairly and professionally in accordance with the best interests of their customers". We fully support EIOPA's view that this principle implies a "customer-centric approach to the use of AI systems", hence the need for "a corporate culture that includes ethics and fairness" embedded in all operations of insurance undertakings, including the deployment and use of AI systems.

We appreciate EIOPA's reminder that "certain pricing practices" are considered non-compliant with the requirement to treat customers fairly: unchecked deployment of AI systems in price optimisation practices should never lead to price discrimination. Insurance undertakings should implement the most rigorous risk management principles

to AI systems that could create risks of discriminations. We also support EIOPA's view in section 3.15 that adequate redress mechanisms should be place for customers to seek redress and note that, for this requirement to effectively increase customer protection, it should come with a requirement for the undertaking and/or intermediary to inform (prospective) customers of any AI system used for the provision of the insurance product they are about to buy and where to find information about said AI system, what data it uses and how it processes them.

Data governance

Q6 - Do you have any comments on the data governance section? What other measures should be considered to ensure adequate data governance of AI systems?

We unfortunately live an in imperfect world where data that is "accurate, complete, representative and free of bias" is often hard to obtain. Nevertheless, the risks to customers depend on the extent of these data imperfections, on the impact that these imperfections have on the output of AI models and on the types of business operations these outputs are used for. It is essential that insurance undertakings provide their relevant staff with the necessary training to identify and understand how imperfect data sets impact model outputs and the risks these entail for customers, as well as the appropriate management structure and incentives to effectively monitor and report biased or erroneous model outputs, especially where those are likely to impact customers.

We believe these requirements should apply most forcefully for AI systems with a potentially significant (direct or indirect) impact on customers (most notably those used in underwriting, pricing and claims handling), while leaving some leeway to undertakings to use less-than-perfect data sets to train AI systems used in ancillary internal processes. The use of such imperfect datasets should, however, be conditional upon undertakings being able to prove that they understand how these imperfections affect model output, implement an effective customer-risk monitoring, human oversight and redress mechanisms. This proportional implementation of the requirements should, naturally, be guided by the outcome of the risk assessment of AI systems.

This tolerance should in any case be limited: there is a limit beyond which the inaccuracy, incompleteness, unrepresentativeness of and biases in a dataset should lead the undertaking to abandon the project of deploying the AI-system.

We furthermore appreciate EIOPA's statement, in section 3.17, that undertakings' data governance policy must be "in compliance with applicable data protection legislation", especially the General Data Protection Regulation (GDPR). "Privacy by design" must be at the core of the development and/or selection of third-party AI systems by an insurance undertaking to ensure that the use of such systems does not violate the rights of customers (and employees).

Documentation and record-keeping

Q7 - Do you have any comments on the documentation and record keeping section? What other measures should be considered to ensure adequate documentation and record keeping of AI systems?

As EIOPA rightly reminds us, keeping adequate and orderly records of insurance undertakings' business, operations and product approval processes are well-established requirements in insurance sectoral legislation. This is a crucial enabler of external review of these operations by supervisors and other interested parties, and of mechanisms through which negatively affected customers and other stakeholders might seek redress.

If the use of AI systems is integrated within these operations, it follows that the documentation and record-keeping requirements also apply to this use of AI systems; this is not a new requirement, merely the logical extension of existing legislation to new processes. We agree that the precise implementation of the documentation and record-keeping requirements needs to be adapted to the specifics of AI-system development and deployment (including specifying the respective obligations of developers and deployers when and where development of AI systems is outsourced), but keeping in mind the end goal of enabling external reviews of operations.

While we generally support a risk-based approach to regulating the use of AI systems and share the objective of reducing the regulatory burden on undertakings, we stress the importance of appropriately documenting all the steps of development and deployment of all AI systems: Without proper documentation, how are supervisors and other interested parties to review the risk assessment conducted by the insurance undertaking?

We note that the industry's push to deploy AI systems in insurance is primarily motivated by cost-cutting motivations and also note that such cost-cutting is most likely to increase the profit margin or insurance undertakings while its effect on the price of insurance products remains to be seen. Therefore, we would kindly like to stress that customers cannot agree for this profit margin increase to be made at their expense and demand that documentation and records be available for review whenever an insurance undertaking chooses to use AI in its operations.

Transparency and explainability

Q8 - Do you have any comments on the transparency and explainability section? What other measures should be considered to ensure adequate transparency and explainability of AI systems?

When it comes to artificial intelligence, we can identify three levels of "explainability". The highest level refers to a firm being able to explain its AI governance, including its choice of AI model(s), the test that is made before deploying it, the limitations that were identified and how these have been mitigated, as well as the ongoing risk-monitoring process that is in place. The intermediate level refers to the firm being able to explain the process through which an AI model produces an output. At the lowest level, "explainability" means the ability to explain how a particular output, a particular decision, was produced by the AI model.

Insurance companies should strive for full explainability, i.e. be able to explain their approach to AI, explain the models used and explain how a particular decision was produced. However, considering the state of AI technology and levels of understanding of AI models, it is unrealistic to expect each and every staff member to be able to explain an AI-based decision to a customer, or even the functioning of a given AI model.

These constraints notwithstanding, the staff of an insurance undertaking that uses AI in its operations should be able to explain to a customer the undertaking's general policy regarding this use of AI and to tell the customer who within the undertaking to ask for more information about an AI-based decision that the customer might find questionable and how to seek redress if necessary. This implies (a) that all staff members that may be in contact with customers have a proper understanding of the firm's policy on the use of AI, including the identification of relevant internal contact points; (b) that the customer is informed that an AI system has been used to produce the decision and (c) that redress mechanisms are in place.

We also note that, where insurance undertakings are not in a position to explain how a given model produces a given output, they should ensure that they remain able to revert to a human processing of the same data used as input to the AI model to compare the human processing with the AI-based one. We consider this an essential element of a robust human oversight system, which is essential for any AI system the use of which could negatively impact customers.

Human oversight

Q9 - Do you have any comments on the human oversight section? What other measures should be considered to ensure adequate human oversight of AI systems?

We fully support EIOPA's proposals on human oversight laid down in section 3.29 of the Opinion. In particular, we support the principle that members of the administrative, management or supervisory body (ASMB) are responsible for the overall use of AI within the organisation. It is our understanding that this responsibility does not require a full knowledge and understanding of the minutiae of each and every AI system used in the insurance undertaking, but a sufficient grasp on the basic principles and concepts to understand the potential risks, as well as access to all the necessary information from within the organisation to ensure that more specialised members of staff are implementing the company's policy in a way that is generally prudent and always compliant with regulatory requirements. We add that the liability of AMSB members related to the use of AI is essential to incentivise these members invest time and effort in its supervision, ensuring that this (increasingly) important part of an undertaking's operations and the operational risk it may entail are effectively subject to senior management oversight.

We fully second EIOPA's call for "sufficient training [to] be provided to staff" in section 3.31, as we agree that sufficient knowledge of an AI system is necessary to be able to detect anomalies such as biased outcomes. This does not necessarily mean that all staff needs to receive a full training on AI; it requires identifying the functions within the organisation that may have to manipulate AI systems (provide input, maintain models, receive outputs) are clearly identified, their specific training needs defined and a policy in place to provide this training.

We note that smaller undertakings may not have sufficient internal (financial and/or human) resources to ensure effective human oversight in all the dimensions listed in section 3.29. Allowing for the outsourcing of functions of AI Officer or Data Protection Officer may be necessary to enable these smaller market participants to reap the same expected benefits of AI as their larger competitors. The Opinion should, however, be amended to lay down supervisory expectations in such cases of outsourcing.

Accuracy, robustness and cybersecurity

Q10 - Do you have any comments on the accuracy, robustness and cybersecurity section? What other measures should be considered to ensure adequate accuracy, robustness and cybersecurity of AI systems?

We support the proposed proportional approach to accuracy, robustness and cybersecurity. If AI systems come to be integrated to essential operations of the insurance undertakings, then undertakings should make sure that these systems will perform consistently and reliably whenever needed.