Response to EIOPA consultation paper on its Opinion on AI governance and risk management

Our reference:	COB-TECH-25-064	Date:	12/05/2025
Referring to:	Consultation paper and impact assessment on EIOPA's Opinion on AI governance and risk management		
Contact person:	Arthur Hilliard, Senior Policy Advisor	E-mail:	hilliard@insuranceeurope.eu
Pages:	6	Transparency Register ID no.:	33213703459-54

CONTEXT, OBJECTIVE AND SCOPE

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

Insurance Europe supports the overall objective of the Opinion, namely "to provide further clarity on the main principles and requirements foreseen in insurance sectoral legislation that should be considered in relation to those insurance AI systems that are not considered as prohibited AI practices or high-risk under the AI Act". However, the context in which this objective is set does not seem appropriate, as it is too broad and applies to too many areas, which risks creating more confusion for insurance companies. While the principles are reflected in insurers' governance and risk management frameworks, some of the examples referred to are not relevant for all AI use cases.

Insurance Europe would stress the importance of explaining the proportionality aspect more granularly by recognising different requirements for: (i) customer-facing versus internal use cases; (ii) deployers versus providers; and (iii) newer AI applications (generative AI) versus machine learning.

The objective of the Opinion should be specifically detailed for each regulation – the Insurance Distribution Directive (IDD), Solvency II and the Digital Operational Resilience Act (DORA). In addition, there is a need to emphasise in the individual sections of the Opinion which requirements derive from which legislation, so that companies are not in any doubt about the scope or which use cases are subject to which requirements. This would provide real support to insurance companies.

The insurance sector already has a very robust regulatory framework (Solvency II, IDD, GDPR, DORA…) that provides sufficient mechanisms and processes to enable insurers to properly manage AI systems and manage their risks. In addition, insurers already have demanding and professional risk management and internal governance systems in place. New obligations or requirements on insurers would not further add to consumer protection and, on the contrary, could severely hamper the ability of insurance undertakings to benefit from innovation.

Insurance Europe notes the statement in paragraph 2.7 that the Opinion "does not set out new requirements and in particular it does not seek to extend the requirements of the AI Act to all AI use cases in insurance". We would question, however, whether in fact this statement is fully reflected in the text of the Opinion. For example, paragraph 3.23 refers to Annex I for an example of the types of records and documentation that should be kept for high-risk use cases, which creates further confusion and seems to run contrary to the statement that the Opinion does not apply to high-risk AI use cases. Moreover, the frequent use of language like "should" goes against the statement that the Opinion does not create new requirements and may in fact mean that supervisory expectations are interpreted more as obligations on insurers. If a given element of the Opinion is not explicitly covered under Solvency II or IDD (or other referenced legislation), it should either be deleted or, as a minimum, clarified that these supplementary elements are merely suggestions that insurers may wish to consider but do not form part of any legal requirements or supervisory expectations. This will help to enhance clarity.

It should also be noted that while the AI Act envisages that national supervisory authorities (NSAs) in the financial sector would serve as market surveillance authorities under the Regulation, some countries have already indicated that they are likely to depart from this approach and designate the Data Protection Authority (or another authority) to oversee compliance with the AI Act. Given that EIOPA's opinion is directed at NSAs, this could lead to dual supervision whereby one authority is competent for high-risk AI systems under the AI Act and another for non-high-risk AI systems that are captured by EIOPA's opinion.

The opinion should use the same terminology in relation to existing legislation (including DORA, IDD and Solvency II) and should particularly avoid introducing new terminology that could potentially lead to misunderstandings or confusion.

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

It is unclear what the exact scope of the Opinion is, specifically whether the intention is:

1. to apply the risk management system of the AI Act for high-risk AI systems to all AI-based use cases employed by insurance companies; or
2. only to those use cases that fall within the scope of the three regulations on which the Opinion is based (IDD, Solvency II, DORA).

Either way, we highlight that the impact in terms of costs and implementation effort would be significant for companies and would, in any case, contradict the risk-based approach of the AI Act.

In terms of clarity of the legal basis, the Opinion should also mention and recognise the fact that Solvency II and IDD have different scopes, which must be taken into account in the different sections of the Opinion (ie Solvency II Art. 41(2): "proportionate to the nature, scale and complexity of operations"; IDD Art. 25(1): "proportionate and appropriate to the nature of the insurance product").

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?*

Insurance Europe would suggest that further consideration be given on how to appropriately ensure that proportionality considerations are taken into account in the opinion. In light of the European Commission's focus on simplification and reducing the burden faced by small and medium-sized companies in particular, including in the application of the AI Act, there is scope to further emphasise this point in the section on proportionality.

Insurance Europe would stress the importance of explaining the proportionality aspect more granularly by recognising different requirements for: (i) customer-facing versus internal use cases; (ii) deployers versus providers; and (iii) newer AI applications (generative AI) versus machine learning.

In addition, the principle of proportionality should be more clearly emphasised and recognised as an indispensable overarching basis for all measures. It should also be reiterated in relation to some of the specific points in the sections that follow, especially in areas where the text approaches the limits of Solvency II and IDD.

More specifically, we would highlight the measures mentioned in the following points:

- **3.3** → Some cited general principles do not appear in the AI Act (eg "large data," "the sensitivity of the data"); additionally, it states that the "potential adverse impact that an AI system could have on the right to non-discrimination" may affect the risk assessment of an AI system. However, any AI system with direct or indirect impact on customers could potentially have such an impact; if this criterion were applied, all such AI systems would have to be classified as high-risk.
- **3.4** → These measures are framed within the context of the insurance sector but should explicitly reference existing sectoral regulations (IDD, Solvency II, DORA).
- **3.5** → The proportionality criterion is vague and undefined.
- **3.5** → In the sentence "measures that ensure responsible use of AI systems", the term "responsible use" should be removed. It is not a formulation or a general requirement that can be established at system level through IDD/Solvency II. Instead, it could state: "[…] undertakings shall develop a combination of proportionate measures that ensure that an AI system operates in accordance with sectoral law. This implies that that governance and risk management measures may be tailored to the specific AI use case [...]."

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?*

The Opinion introduces prescriptive language throughout, effectively creating obligations that extend beyond mere clarification of existing sectoral legislation. For purposes of clarity, the Opinion should clearly state which regulation each element is based on. It should also be clear which elements fall within the scope of the various regulations, and when elements are outside the scope and presented only as recommendations.

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?*

As it is written, it appears that the entire section applies exclusively to the scope defined in point 3.11. We request confirmation of this interpretation.

We would also question the reference "free of bias" in paragraph 3.13, given than it seems unrealistic to have data sets completely free of bias. Requiring data (which will be used to train or operate a model) to be free of bias *a priori* is a high bar to pass, as the bias may only be discoverable after the model has performed its actions over the data, or through assessment of the outcomes of the model relative to the objective in an operational context. Developers and operators should be encouraged to assess for potential bias outcomes as early as makes sense given the data, model and objective, and frequently once deployed. Firms would then need to address any biases found, should it be appropriate, in order to encourage the use of these models without unduly putting customers at risk. The reference to "free of bias" should therefore be removed or at a minimum should make reference only to "unwanted bias".

We welcome the attempt to present fairness metrics in Annex I, but unfortunately no specific reference to the insurance industry can be recognised. As a result, the added value of this list must be questioned. We suggest the deletion of this reference.

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?*

As it is written, it appears that the entire section applies exclusively to the scope defined in point 3.16. We request confirmation of this interpretation.

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?*

EIOPA suggests that undertakings should keep appropriate records of the training and testing data and the modelling methodologies. This should not apply to AI systems procured from third party providers given that the insurance undertaking will not be in a position to have this data. Deployers do not always have access to all the information that EIOPA is suggesting (eg datasets used for training, the code on which the system is based). It would be important therefore to distinguish between the roles of AI deployers and providers and consider separate record-keeping expectations. When insurance undertakings deploy AI systems or models procured from third parties, it should be sufficient to take reasonable steps to obtain relevant information from the AI system providers, who are legally required to share transparency-related documentation about their products.

With regard to paragraph 3.23, Annex I is clearly introduced as an example of the types of records and documentation. For this reason, an alternative wording than "should" would be preferable to clarify the status of Annex 1 as an 'example' only.

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?*

As it is written, it appears that the entire section applies exclusively to the scope defined in point 3.24. We request confirmation of this interpretation. Paragraph 3.24 references both Solvency II and DORA as a legal basis. To avoid unnecessary burdens by extending the scope of these regulations to use cases that are out of scope and to add legal clarity, the specific elements/considerations in the section should be clearly marked as to whether they apply in light of DORA or Solvency II.

Transparency and explainability are key elements to facilitate improved public understanding and trust regarding the use and application of AI. Ensuring clarity as to when AI is being used and for what purpose will not only help to enhance consumer trust in the technology but also facilitate its overall uptake by industry. The provision of meaningful, easy-to-understand information will also contribute positively to more informed choices for consumers.

However, it should be noted that, the domain context and use case are important factors in determining what kinds of explanation firms should be able to provide. The most appropriate way of explaining decisions made by AI is highly dependent on the context (ie the significance of the outcome) and the severity of the consequences in the event that an erroneous or inaccurate outcome has been arrived at, in line with the principle of risk-based proportionality. In some cases, requiring certain kinds of explainability may have an impact on the accuracy and performance of the AI system, or create privacy or security implications. For example, a company using AI for fraud detection purposes should be able to decide not to share information or provide explanations about the model or data it uses to certain audiences, in light of concerns over model manipulation or exploitation. However, a 'responsibility' or 'safety and performance' explanation may still be required for certain audiences, such as auditors, or a denied claimant might require a 'fairness' explanation. The UK Information Commissioner's Office and the Alan Turing Institute published 'Explaining Decisions made with AI' in 2020, which provides practical advice on explaining decisions made by AI systems. We consider that EIOPA could leverage this document and the expertise of these two organisations as best practice in defining 'explainability' and providing guidance for firms navigating context-dependent explainability.

Moreover, there will be a need for greater flexibility when it comes to explainability in the context of generative AI use. For example, large language models (LLMs) are often not explainable as to *why* the model made a particular choice in simple human-understandable terms. Therefore, a strict explainability requirement for such models could hinder the deployment of generative AI. This should also be reflected in the Opinion.

The focus of any principles on transparency and explainability should therefore be on providing meaningful information and clarity about the AI system and its decisions or recommendations to facilitate greater consumer understanding and give them more clarity and control over their data subject rights when personal data is being processed by the AI system.

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?*

While Insurance Europe fully recognises the importance of human oversight, it should be acknowledged in the opinion that human oversight is sufficient at the system level (human on the loop) and does not need to be implemented for every single-run process (human in the loop), in order to still allow for automation of processes. The Opinion should allow for automated oversight mechanisms for low-risk applications, with human intervention reserved for material decisions or anomalies.

EIOPA suggests that administrative, management or supervisory body (AMSB) members are responsible for defining and internally communicating the vision and policy towards AI within the organisation. This should be the responsibility of the executive managers – not the AMSB which generally has an oversight function and will not "internally communicate the vision and policy" towards AI. The proportionality principle should also be taken into account at the level of AMSB engagement.

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?*

Insurance Europe would propose introducing the term “where appropriate” in paragraph 3.34 when referring to the use of metrics.

Traditional accuracy metrics are not useable in the case of generative AI models, as answers to the same question can differ for each query. It is not possible to directly measure accuracy in percentage terms for a test dataset – or via random samples – as with traditional AI.

Paragraph 3.32 references both Solvency II and DORA as a legal basis. To avoid unnecessary burdens by extending the scope of these regulations to use cases that are out of scope and to add legal clarity, the specific elements/considerations in the section should be clearly marked as to whether they apply in light of DORA or Solvency II.

Insurance Europe is the European insurance and reinsurance federation. Through its 39 member bodies — the national insurance associations — it represents insurance and reinsurance undertakings active in Europe and advocates for policies and conditions that support the sector in delivering value to individuals, businesses, and the broader economy.