European Insurance and Occupational Pensions Authority

EIOPA-BoS-25-362
06 August 2025

Resolution of comments - Opinion on Artificial Intelligence Governance and Risk Management

Introduction

The European Insurance and Occupational Pensions Authority (EIOPA) would like to thank all the participants in the public consultation for their comments on the draft Opinion on Artificial Intelligence Governance and Risk Management (hereinafter "the Opinion").

The contributions received provided important input and guidance to aid EIOPA in finalising the Opinion. All the comments submitted were given careful consideration. This document contains the non-confidential individual comments received and EIOPA's response to them. For further details please also refer to the Feedback Statemen of the public consultation published as a separate document.

Resolution of comments

No.	Name of the stakeholder	Q1 - Do you have any comments on the context and objectives of the Opinion?	EIOPA's comments
1	Mirko Kraft	EIOPA's consultation on an Opinion on Artificial Intelligence Governance and Risk Management is welcomed (EIOPA 2025). It is important that also insurance supervisors address the risks that are related to or increased by AI systems used by insurance companies, especially if advanced AI systems are used extensively in core insurance functions such as underwriting, pricing, and claims management. AI systems may generate or increase risks that require proper oversight, taking into account to what extent the business of an insurance undertaking relies on AI systems and focusing on risk prevention (e. g. "ethical AI by design"). Supervision should not mean waiting for scandals and breaking the law, because trust in insurance companies is important. This includes taking into account the sustainability issue caused by AI, e.g. the CO2 emissions.	Noted. The Opinion does not create new requirements and does not alter the scope of insurance legislation mentioned therein. The Opinion follows a principles-based approach and highlights the key principles that need to be observed when using AI systems, taking into account risk-based and

		It has to be taken into account that the use of AI systems varies in the insurance industry: InsurTech as big traditional big players might build up their future business models on them. Contrary to the approach suggested by EIOPA (1.3) it is recommended that insurance companies and intermediaries are addressed separately, because the legal basis for supervising them is different and mixing it up is confusing and might create new requirements without legal basis. Also the wording in the consultation paper is misleading as it refers to both as "undertakings". It is worth mentioning that EIOPA is not mandated by the AI Act to address the issue of AI governance and risk management of (insurance) undertakings. It seems appropriate to put also references into other legal texts that are more binding. It is imperative to acknowledge that even in ostensibly low-risk AI systems, there is an inherent risk of consumers being disconnected from essential services if they are unable to contact a human representative of the insurance company when the AI-based system fails to comprehend their request. In a manner analogous to the digitalisation of information disclosures, which is accompanied by the right to access physical documentation, it is essential that the integration of AI systems in firm-consumer interactions is accompanied by the right to human contact. This right must be both readily apparent and easily accessible. It is not sufficient that EIOPA will look into the supervisory practices of competent authorities after two years after publication of the opinion, because AI is developing very fast and requires ongoing monitoring. EIOPA should also extent its research capabilities in this area.	proportionality considerations. EIOPA will indeed continue monitoring the AI-related developments in the insurance sector, such as with the on-going market survey on Generative AI.
2	BIPAR	BIPAR welcomes the objective of EIOPA's Opinion to help navigate the interplay between the EU AI Act and applicable insurance legislation. In point 1.3, it is explained that the Opinion covers the activities of both insurance undertakings and intermediaries insofar they may use AI systems within their respective areas of competence in the insurance value chain. They are jointly referred as "undertakings" in the Opinion. However, it seems that this Opinion is mainly focused on insurers/ manufacturers (including intermediaries when manufacturing insurance product for sale to customers). Under SII, IDD (level 1 and 2), DORA etc…, the obligations of insurers and intermediaries (and/or manufacturers/distributors) are different – in some cases micro and SME intermediaries are not in scope - and we believe that this should be clarified where	Noted. The Opinion has clarified that the reference to articles from Solvency II, DORA, and IDD, which are not exhaustive, do not affect their scope of application. However, the principles outlined in the Opinion (e.g., fairness, human oversight, data management etc.) remain applicable to the use of AI systems in insurance. For example, data governance

		appropriate in the Opinion (ex : point 3.4 and 3.5 and others) to avoid confusion. We welcome the objective of EIOPA to further provide clarity on the following aspects: - definition of AI systems with specific focus on insurance AI use cases; and - navigating non-high risk AI systems as per the definition of the EU AI Act. We would appreciate that the Opinion also provides clarity on the following: - use cases for the insurance distribution industry; - use cases in the captive insurance industry; and - navigating the EU AI Act to ensure that the system used is not considered to be a high risk AI system. We believe it useful if EIOPA provides more clarity on when certain use cases could stray into being classified as a high risk AI system. Analysis should be undertaken regularly. It is reasonable to expect significant evolutions in the adoption of AI systems and, therefore, the scope of EIOPA's Opinions may extend in the future - especially based on real-business use case - to showcase how specific application of AI systems are being seen through the regulatory and supervisory lens. We also believe that in paragraph 28, references should also be made to the European Commission guidelines on AI system definition (see https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application). Reference should also be made also to the Commission's guidelines on prohibited artificial intelligence (AI) practices (see https://digital-strategy.ec.europa.eu/en/library/).	is fundamental to ensuring that consumers are treated fairly. The Opinion now includes a reference to the European Commission's Guidance on the definition of AI system. EIOPA will continue monitoring market developments via different tools in close collaboration with stakeholders, and it envisages to subsequently develop more detailed analysis on specific AI systems or issues arising from the use of AI systems in insurance and provide further guidance, if appropriate.
3	AFPA, Austrian Financial & Insurance Professionals Association	Die EIOPA erwähnt in diesem Absatz das Erfordernis von, durch die Unternehmen zu entwickelnden Governance- und Risikomanagementgrundsätzen, bei denen auch risikobasierte und verhältnismäßige Erwägungen berücksichtigt werden sollen. Durch die teilweise thematisch sehr ähnlichen Anforderungen der verschiedenen Regularien, muss eine einheitliche Linie bei der Auslegung der Anforderungen, unter Zuhilfenahme	Noted. EIOPA agrees with the need to avoid double regulations; The Opinion aims to provide guidance on how different provisions

		bestehender Synergien, seitens der Aufsicht gewährleistet werden. Es dürfen nicht gleichgelagerte Anforderungen in unterschiedlicher Intensität und Qualität geprüft und bewertet werden. Die Ziele sind grundsätzlich sinnvoll, da es Klarheit für nicht-hochriskante KI-Systeme gibt, und Doppelregulierungen vermieden werden. Wichtig ist ein Fokus auf Innovation und Bürokratieabbau, da die Versicherungs-wirtschaft bereits stark belastet und reguliert ist. Trotzdem scheinen die formulierten Ziele teilweise zu abstrakt formuliert. Insbesondere die Zusammenarbeit mit dem KI-Büro der Europäischen Kommission muss zahlreiche synergetische Lösungen liefern. Immens wichtig werden wohl die, unter 4.3. erwähnten, geplanten Leitlinien. Es wird angeregt, die Analysen zu KI-Anwendungsfällen und /oder –Problemen bereits umgehend zu starten um nicht erst nach zwei Jahren, sondern von Beginn an, Unterstützungsleistungen durch Veröffentlichungen und Leitlinien zur Verfügung zu stellen. The EIOPA mentions in this paragraph the requirement for companies to develop governance and risk management principles, which should also consider risk-based and proportional considerations. Due to the partially very similar thematic requirements of the various regulations, a consistent line in the interpretation of the requirements must be ensured by the supervisory authority, utilizing existing synergies. Similar requirements must not be examined and evaluated with different intensity and quality. The goals are fundamentally sensible, as they provide clarity for non-high-risk AI systems and avoid double regulations. It is important to focus on innovation and reducing bureaucracy, as the insurance industry is already heavily burdened and regulated. Nevertheless, the formulated goals seem partially abstract. In particular, the collaboration with the AI office of the European Commission must deliver numerous synergistic solutions. The planned guidelines mentioned under 4.3 will probably be immensely important. It is suggested to start the analyses of AI use cases and/or problems immediately, so that support services through publications and guidelines are available from the beginning and not only after two years.	of insurance sector legislation should be interpreted in the context of AI systems. EIOPA also acknowledges the importance of collaboration with the European Commission's AI Office and other competent authorities. This is the approach EIOPA has taken so far and will continue to pursue going forward. EIOPA will continue monitoring market developments via different tools, and it envisages to subsequently develop more detailed analysis on specific AI systems or issues arising from the use of AI systems in insurance and provide further guidance, as relevant.
5	Insurance Europe	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	Noted. The Impact Assessment accompanying

		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	the Opinion concluded that EIOPA should focus on providing high level guidance based on existing legislation. At a later stage EIOPA may provide more detailed guidance for specific uses of AI system in insurance, where relevant. The Opinion does not create new requirements and does not alter the scope of insurance legislation mentioned therein. EIOPA has emphasized the importance of a risk-based and proportionate approach, and has included references to the need to follow this approach in each of the principles outlined in the Opinion, which should help to provide clarity on the proportionality aspect. The Opinion now also includes further examples of the criteria that could be included in the impact assessment, such as the differentiation between internal uses and consumer-facing applications, or the number

		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.	of retail customers affected. The scope of the Opinion covers AI systems used in insurance that are not considered prohibited AI practices or high-risk under the AI Act, in order to avoid creating unnecessary overlaps and regulatory burdens.
6	Swedish Insurance trade union Forena	Initial Comment - objectives and context We welcome EIOPA's initiative to seek input on its Opinion on AI governance and risk management. The recognition that responsible AI deployment requires inclusive and transparent governance is a significant and timely step. As highlighted in the ISSDC Joint Declaration https://uniglobalunion.org/news_media/uploads/2021/03/20210316_issdc_joint_declaration_on_artificial_intelligence_final.pdf, agreed by European insurance sector employers – Insurance Europe, BIPAR and AMICE – and employees – UNI Europa Finance – social dialogue and a "human-in-control" principle must be integral to any trustworthy AI system. Workers are not only affected by AI—they also hold critical insights into how these systems function in real-world settings and how they can be improved to support fair and effective outcomes. Experience from the Swedish insurance sector, including findings from Forena's 2023 report "Strukturomvandlingen i försäkringsbranschen med fokus på AI och automation", shows that AI systems are increasingly used in areas such as claims handling, customer interaction, fraud detection, underwriting, and compliance. These systems are reshaping job roles, decision-making processes, and skill requirements.	Noted. EIOPA acknowledges the importance of social dialogue and has explicitly mentioned this possibility in the text of the Opinion. The Opinion also emphasises the need to develop adequate training for relevant staff.

		While many employers have ambitious digital strategies, Forena highlights a lack of transparency and limited employee involvement in the risk management and implementation of AI. Workers often report uncertainty about how AI is used, how their work is affected, and how they are evaluated in AI-enhanced environments. When involvement lacking early in the AI deployment and implementation process, there is a risk of resistance and mistrust, which also means a financial risk. Local trade unionists often experience being presented with finalized decisions and ready-made systems, with no real opportunity to influence their development. This undermines both the efficiency and legitimacy of the process and the productive outcome of AI tools. However, where there is a functioning local social dialogue and unions are involved from the beginning, they can act as ambassadors for digital change. That is in trade unions' interest—if strategic changes such as new AI are handled through trust and collaboration. Employee involvement and the voice of trade unions facilitate smoother implementation, strengthen employee understanding and adaptation, and often result in more cost-effective and successful outcomes. Social dialogue fosters sustainable business development and mitigates financial risks associated with AI investments. Trade unions can also serve as sounding boards for pilot testing and rollout, drawing on networks across companies to share experiences and insights. Finally, employers should not forget to include workplace safety representatives and local health and safety organizations, who can provide valuable perspectives on AI-systems impact. For Forena, ethical and human-centric AI is essential. We see a need for co-determination, the right to information and consultation, and safeguards against de-skilling and intensification of Klassificering: Publik information work. It is essential that employees are given opportunities for competence development and that new technologies are introduced through negotiation and trust-based collaboration. Without active social dialogue —either at the workplace or at the national level—AI risks undermining job quality and creating new accountability. We support EIOPA's focus on risk-based, proportionate regulation and encourage an inclusive approach on social dialogue as a guiding principle. AI risk management in insurance should ensure that new techniques enhance—not erodes—human dignity, rights,	

		and expertise, and that it is implemented through transparent, negotiated processes aligned with core European values.	
7	Lloyd's Market Association	We welcome the Opinion and its objective. We also strongly support the principles based, high level guidance approach taken in this paper and the intention to not set out new requirements as set out in paragraph 2.7. We are also pleased that this Opinion recognises the fact that a lot of the scope of the Opinion is already covered by existing regulation, such as Solvency II, DORA, IDD and GDPR. There are various points in the Opinion where we feel that the principles based approach may have been inadvertently strayed from and we point these out in the answers to the questions that follow.	Noted. The Opinion emphasises the importance of following a principles-based, risk-based and proportionate approach to the use of AI systems. For example, the Opinion now includes references to the need to follow this approach in each of the principles outlined in the Opinion, which should help to provide clarity on the proportionality aspect.
8	AMICE	AMICE supports the objectives of EIOPA's Opinion and the intention to provide guidance to supervisors. Indeed, while most AI systems used by insurance companies are deemed to be low-risk under the AI Act, certain AI systems employed in core segment of the insurance value chain may present risks that require monitoring and mitigation. We agree with the decision to provide a general opinion for supervisors, rather than to set out new detailed requirements for insurers, as the applicable EU regulations are already extensive and robust. Nevertheless, the use of prescriptive terms (such as term "should") risks introducing de facto requirements for insurers, which could contradict the original purpose of the Opinion. This could inadvertently extend the applicable requirements thus discouraging the adoption of AI. Therefore, we suggest following a principle-based approach and removing terms like "should" that may impose direct obligations on insurers.	Noted. The Opinion does not create new requirements and does not alter the scope of insurance legislation mentioned therein. The Opinion follows a principles-based approach and highlights the key principles that need to be observed when using AI systems, taking into account risk-based and proportionality considerations.
9	Institute of International Finance	We support that the Opinion is addressed to competent authorities rather than directly to undertakings (para 1.3), which is appropriate for guidance of this nature. We appreciate that the Opinion acknowledges AI's 'significant opportunities' for the insurance sector (para 2.2), and think the Opinion could go further in this respect. AI systems can meaningfully enhance consumer protection and market stability through improved fraud detection, enhanced pricing, customer segmentation and risk modeling capabilities, and the	Noted. The Opinion does not create new requirements and does not alter the scope of insurance legislation mentioned therein. The use of terminology such as

		potential for automated and faster claims management. Requirements vs guidance We strongly welcome the statement that 'This 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' (para 2.7). However, in our view, the Opinion is not true to this description of purpose and explicitly adds new requirements and quasi-requirements directly on insurers, in many instances using prescriptive language such as 'undertakings should' (13 instances), and many other prescriptive statements including 'Administrative, management or supervisory body (AMSB) members should,' 'compliance and audit functions should', 'the Data Protection Officer should', etc. The Opinion states it aims to provide 'further clarity on the main principles and requirements' in insurance sectoral legislation (para 2.6), but appears to introduce prescriptive language throughout, creating de facto obligations that go beyond clarification. This prescriptive language is, in our submission, not appropriate for an Opinion that does not purport to extend requirements and also is addressed to competent authorities and not to undertakings or intermediaries. Definition of AI system We welcome that the Opinion is based on the definition of AI systems adopted in the AI Act, ensuring consistency at the European level (para 2.8). Dueling taxonomies is a very real and challenging possibility. As such, it is essential to provide a clear and precise definition of the concept of AI that is fully aligned with the established definition in the AI Act. This will help ensure that all stakeholders have a common understanding of the scope of AI. The objectives should acknowledge that existing insurance sectoral legislation already requires adequate and proportionate governance and risk management measures when using mathematical models, regardless of whether they are considered AI systems or not. Timing and coordination We are concerned about the timing of this Opinion, coming shortly after the European	"should" is common in similar guidance documents developed by EIOPA in the past. The Opinion does not establish a supervisory checklist, but rather it follows a holistic approach to AI governance and risk management anchored in risk-based and proportionality considerations. The Opinion is based on the definition of AI systems of the AI Act. The Opinion now includes an explicit reference to the European Commission's Guidelines on the AI system definition. The Guidelines include explicit references to linear and logistic regression models. EIOPA also acknowledges the importance of collaboration with the European Commission's AI Office and other competent authorities, taking into account their respective work to ensure coordination and avoid duplications and unnecessary burdens.

		Commission's consultation on targeted guidance on the AI Act with regard to the financial services sector. We note that there is also an ongoing process of iterative consultation around the development of rules for general-purpose AI systems. In our view, there is a risk of overlapping and duplicative requirements, and a strong case for EIOPA to delay finalization of its opinion, pending completion of all rule- and guidance-making processes under the EU AI Act. To do otherwise would be to risk misalignment between requirements or guidance finding their origin in the EU AI Act, and that emanating from EIOPA. Our members are also concerned about a perceived lack of coordination between relevant authorities under the AI Act at both EU and national levels, particularly with respect to definitions and reporting requirements. We recommend maximum coordination between EIOPA and the EC's AI Office. Coordination of reporting requirements across all public bodies responsible for supervising AI will avoid duplicative efforts and ensure consistency in approach.	
10	Gesamtverband der Deutschen Versicherungswirtschaft	- The European Commission has made strengthening competitiveness a priority, including by reducing bureaucracy and barriers to innovation. This is also emphasised in the EU AI Continent Action Plan. For example, it states that the EU and member states should first focus on the effective implementation of the AI Act and gain experience with its implementation before considering new legislation for AI. In order to achieve these goals in practice, this approach should also be supported by regulation. - We welcome the clarification in section 2.7 that the consultation paper does not establish new requirements, particularly the clarification that it does not aim to extend the scope of the AI Act to all AI applications. We therefore interpret the opinion as a compilation of existing insurance industry legislation (e.g. IDD and DORA) in the context of the use of AI. - We also endorse the principle of proportionality, as well as the use of the AI definition in the AI Act. - The opinion should use standardised terminology in relation to existing legislation (including DORA, IDD and Solvency II) and, in particular, should not introduce new terminology that could potentially lead to misunderstandings or ambiguities. - There are doubts as to whether the intention stated in section 2.7 not to introduce any new requirements is actually upheld throughout the opinion. In our view, the large number of prescriptive statements ('Insurers should...' etc.) carries the risk of the supervisory authority	Noted. The Opinion does not create new requirements and does not alter the scope of insurance legislation mentioned therein. The use of terminology such as "should" is common in similar guidance documents developed by EIOPA in the past. The Opinion does not establish a supervisory checklist, but rather it follows a holistic approach to AI governance and risk management anchored in risk-based and proportionality considerations. The Opinion is based on the definition of AI systems

		establishing new 'quasi-requirements' as well as resulting in parallel regulation to the AI Act. In particular, 'breaking down' of the boundaries between high-risk and non-high-risk AI should be avoided at all costs. Such developments would undermine the risk-based approach of the AI Act and would be entirely disproportionate to the actual risks of non-high-risk AI. In the long term, this would hamper AI-driven innovations. - Furthermore, the timing of the publication of the opinion is worth questioning, given that the European Commission is still working on guidelines for the practical implementation of the AI Act.	of the AI Act. The Opinion now includes an explicit reference to the European Commission's Guidelines on the AI system definition. The Guidelines include explicit references to linear and logistic regression models. EIOPA recognises the value of collaborating with the European Commission's AI Office and other relevant authorities to ensure a coordinated approach, avoid duplication of efforts, and prevent unnecessary regulatory burdens. This collaborative approach is already being implemented by EIOPA and is expected to continue in the future.
11	CNP Assurances	CNP Assurances supports the overall objective of the opinion, namely "to provide clarification on the main principles and requirements provided for in insurance sector legislation that should be taken into account in relation to insurance AI systems that are not considered prohibited or high-risk AI practices under the AI Act". However, the opinion is too broad and applies to too many areas, which risks might lead to uncertainty for insurers. The objective of the opinion should be specified for each regulation (Solvency II, IDD, DORA) and propose operational recommendations on the governance of AI systems and the management of the risks associated with them. Further clarification on the distinctions between AI systems and traditional actuarial models is needed. Additionally, considering all insurance branches affected by AI would make the opinion more applicable to the sector.	Noted. The Impact Assessment accompanying the Opinion concluded that EIOPA should focus on providing high level guidance based on existing legislation. At a later stage EIOPA may provide more detailed guidance for specific uses of AI system in insurance, where relevant.

		Regarding the statement in paragraph 2.8, it appears challenging to apply the same risk governance principles to AI algorithms as those used for traditional mathematical models. A clear delineation of the minimum requirements necessary to ensure appropriate monitoring of these risks would be beneficial.	The Opinion is based on the definition of AI systems of the AI Act. The Opinion now includes an explicit reference to the European Commission's Guidelines on the AI system definition. The Guidelines include explicit references to linear and logistic regression models.
12	IRSG	We appreciate EIOPA's initiative and its stated objectives. Although most of the AI systems deployed by insurance undertakings are neither prohibited nor classified as "high-risk" by the AI Act, advanced AI systems extensively used in core insurance functions such as underwriting, pricing, and claims management may generate or increase risks that require proper oversight, taking into account to what extent the business of an insurance undertaking relies on AI systems and focusing in risk prevention (e. g. "ethical AI by design"). Also, we agree on the choice of issuing a high-level opinion addressed to supervisors, instead of detailed guidance addressed to insurance undertakings, and on the need to not add further requirements, considering that the existing EU normative framework – Solvency II, IDD, GDPR, DORA, and now the AI Act itself – already constitutes one of the world's most comprehensive and robust regimes. These prescriptive regulations provide adequate tools to authorities and insurance undertakings for supervising, managing, and mitigating AI-related risks effectively. AI is not a new instrument for undertakings, and its recent evolutions can be well governed within the existing governance and risk management arrangements, which are comprehensive and robust. Introducing additional detailed requirements would risk overlapping or contradicting existing rules, creating complexity without clear benefit to client protection. While welcoming EIOPA's stated objective to avoid imposing new mandatory requirements, we are concerned by the Opinion's frequent use of prescriptive language (particularly the term "should"), which implies obligations of results and ambitious objectives for insurance undertakings. This approach not only contradicts the Opinion's agreeable premises and stated objectives but also results in additional prescriptive requirements, as it sets new supervisory expectations for insurers to meet. It would be good if, in general, the term 'should' were not used when no new obligations are being imposed, as it is misleading.	Noted. The Opinion especifies that it does not establish new requirements. The use of terminology such as "should" is common in similar guidance documents developed by EIOPA in the past. The Opinion does not establish a supervisory checklist, but rather it follows a holistic approach to AI governance and risk management anchored in risk-based and proportionality considerations. The Opinion explicitly integrates the principle of proportionality in each of its sections. EIOPA also acknowledges the importance of social dialogue and has explicitly

		Expressions that allude to a recommendation rather than an obligation are more appropriate. Experience demonstrates that overly prescriptive requirements impose disproportionate burdens, stifling innovation and limiting EU insurers' competitiveness. Overly stringent obligations could ultimately harm consumers, reducing market competition and the availability of beneficial innovations. This outcome directly conflicts with the current EU political agenda, which places competitiveness and innovation as paramount objectives to be pursued. Therefore, we strongly recommend revising the language of the Opinion to fully align with its stated objectives and avoid surreptitiously introducing new mandatory requirements in addition to those already applicable. A principle-based approach, focused on consumer outcomes, is essential for allowing insurance companies to innovate, evolve their offerings and achieve efficiencies which will also benefit their customers. Specifically, we propose: (i) eliminating prescriptive references ("should" formulations) addressed directly to insurers; (ii) consistently adopting consumer-outcome-focused language; and (iii) explicitly integrate the principle of proportionality in each of the areas object of recommendations, as suggested in the following answers. A proportionate, risk-based, and outcomes-focused approach will enable insurers to responsibly deploy innovative AI systems, thus enhancing product offerings, operational efficiency, and consumer welfare, while ensuring adequate mitigation against material risks. In relation to the approach, we are worried that the current wording makes the consumer-outcome focus appear merely as a justification for principle-based (which some might interpret as "light-touch") regulation. From our perspective, it is essential to remind that, even in seemingly low-risk AI systems, there is an inherent risk for the consumer to be cut-off from essential services if they are not able to reach a human representative of the insurance undertaking when the AI-based system fails to understand the consumer's request. Just like digitalisation of information disclosures need to come with a right to access to paper, the use of AI-systems in firm-consumer interactions must come with a right to a human contact (and that right must be obvious and easy to exert). In addition, we think that the objectives should explicitly recognize employees and trade unions as key stakeholders in AI systems. Employees provide unique insights into operational risks and can enhance both design and implementation through early involvement. Social dialogue at all levels is vital to ensure that AI systems are implemented responsibly. By addressing employment aspects of AI, this Opinion lay a groundwork for both innovation and a sustainable workforce.	mentioned this possibility in the text of the Human Oversight section.

13	CRO Forum	Thank you for the opportunity to provide comments on the Opinion. The CRO Forum produced an internal paper on AI Risk Management at the end of 2024. The responses provided here draw heavily on the key themes from that paper. Once finalised the Opinion and Impact Assessment will provide timely support for supervisors and insurers as they consider the evolving threats and opportunities of AI at insurance firms and how they can supervise or manage the risk associated with them in a proportional way, balancing the need to encourage innovation and embracing opportunity with maintaining financial stability and managing risk. While robust supervision of AI is important, care should be taken not to stifle innovation and economic progress at this early stage of AI adoption in insurance. The marketplace has historically shown the ability to self-regulate during technological transitions, as evidenced by the evolution of IT governance in insurance. This is particularly important given: o The competitive pressure from other markets (US, China) with significant AI investments o The need for European insurers to maintain competitiveness through efficiency gains o The industry's established practice of parallel human oversight and business continuity planning o The risk that excessive early regulation could disadvantage regulated markets In our view, the EIOPA should continue to consult with the full range of regulatory and statutory bodies to ensure that the requirements for firms for risk management from these bodies remains joined up and non-contradictory. Overtime EIOPA could consider how supervisors may support and oversee the work of insurers to understand the emerging risks from AI, while recognizing that supervisory approaches may vary across jurisdictions based on existing risk management frameworks. Many jurisdictions follow a principles-based, technology-neutral approach, where AI risks are addressed through existing governance and risk management requirements. While certain emerging risks (such as over-investment, silent AI coverage, overconfidence in AI) warrant attention, their supervision should be proportionate and consider: o Existing regulatory frameworks and their effectiveness o The materiality of AI applications o The probability of risks materializing o Sector-specific characteristics	Noted. The Opinion emphasises the importance of following principle, risk-based and proportionate approach to the use of AI systems. EIOPA will continue monitoring the AI-related developments in the insurance sector in close collaboration with stakeholders. For example, it has recently issues market survey on Generative AI. In the future it may develop further guidance for specific uses of AI systems or issues arising from them, as relevant. EIOPA also supports global alignment on these issues, for instance by supporting the recent Application Paper on Artificial Intellgence developed by the International Association of Insurance Supervisors. Regarding the reference to sandboxes, EIOPA already active participates in the European Forum of Innovation Facilitators (EFIF), and will closely

		This allows for controlled integration of AI technologies while maintaining effective risk management and supervision. Further actions for a controlled introduction and implementation of AI can be: • Encouraging Collaboration: Encouraging collaboration between insurers and technology providers to ensure that AI systems are developed and implemented in a way that aligns with regulatory expectations and industry best practices. • Global Alignment: Emphasising the importance of aligning EIOPA's Opinion with other global regulatory frameworks to ensure that European insurers can operate seamlessly in international markets. • Innovation Sandboxes: Suggesting the establishment of regulatory sandboxes where insurers can test AI applications in a controlled environment before full-scale deployment, helping to identify and mitigate risks early.	follow the establishment of AI sandboxes foreseen in the AI Act.
14	European Financial Congress	EIOPA's opinion makes it clear that its goal is to clarify how to apply existing sectoral regulations (Solvency II, IDD, DORA) in the context of AI, which were not widely used in the enactment of these regulations. Additionally, the idea is to promote supervisory consistency and uniform practices across the EU, while emphasizing consumer protection and preventing regulatory arbitrage. It is worth noting, however, that while the Opinion does not formally introduce new requirements, it can lead to increased administrative obligations and implementation costs for the insurance industry, especially for smaller players, due to high-level supervisory expectations and recommendations for documentation, risk assessment and regular reviews. This could negatively affect the competitiveness of the industry if clear guidance is not provided on the proportionality and practical implementation of these rules.	Noted. The Opinion does not create new requirements and does not alter the scope of insurance legislation mentioned therein. The use of terminology such as "should" is common in similar guidance documents developed by EIOPA in the past. The Opinion does not establish a supervisory checklist, but rather it follows a holistic approach to AI governance and risk management anchored in risk-based and proportionality considerations.
15	European Confederation of Institutes of Internal Auditing	We have some doubts about the role of EIOPA in defining common supervisory stand-ards/interpretations on a cross-sector EU Regulation (i.e., AI Act), that locally will fall under re-sponsibility of non-insurance regulators (e.g., ACN, not IVASS, in Italy):	Noted. The scope of the Opinion covers AI systems used in insurance that are not considered prohibited

		o What is the objective of this opinion? o Will the opinion provided by EIOPA be binding for the local regulators?	AI practices or high-risk under the AI Act, in order to avoid creating unnecessary overlaps and regulatory burdens. Moreover, the Opinion aims at providing guidance of how insurance regulation (i.e. not the AI Act) should be implemented in insurance, which is the competence of insurance regulators.
16	BETTER FINANCE	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.	Noted.
17	Actuarial Association of Europe	Key message: The AAE supports EIOPA's principle-based and proportionate approach. We would welcome, however, greater clarity on the boundary between AI systems and traditional actuarial models. Moreover, a broader reflection on other areas of insurance impacted by AI would help ensure the Opinion's relevance across the sector. Detailed response: We welcome the pragmatic and proportionate approach taken in the Opinion, which aligns well with the framework set out in the AI Act and avoids introducing unnecessary additional requirements. This provides a strong basis for the insurance sector to adopt AI responsibly while preserving flexibility across a diverse European market. We particularly value EIOPA's commitment to a principle-based framework. Such an approach allows for appropriate tailoring across various business models and product types in the European insurance landscape, and we believe this is key to maintaining both	Noted. EIOPA has included more examples of uses of AI systems across the insurance value chain. The Opinion now also includes an explicit reference to the Commission's Guidelines on AI system definition where linear and logistic regression are referenced. EIOPA acknowledges that further guidance may be provided in the future in this regard.

		innovation and consumer protection. It might be helpful for EIOPA to consider expanding the scope of examples provided to better reflect the breadth of AI use across the insurance value chain. For instance, there are areas beyond life and health underwriting where AI systems may pose significant risks, such as in automated claims handling or pricing in property and casualty insurance. These can also impact fairness and customer outcomes. Some uncertainty remains in the market regarding the boundary between AI systems and traditional statistical models, such as Generalised Linear Models (GLMs). While we recognise that traditional GLMs are generally considered outside the AI Act's definition, we believe it could be helpful for EIOPA to confirm this distinction and clarify expectations where such models are embedded in more complex or partially automated systems. This would support consistent interpretation and proportional application of governance requirements. Looking ahead, we suggest it might be helpful for EIOPA to consider how the Opinion could remain adaptable over time. As AI systems evolve rapidly, future developments may introduce new risk dimensions or shift the context of existing applications. Ensuring that governance frameworks are sufficiently forward-compatible would help maintain their relevance and effectiveness.	The principles-based nature of the Opinion and its emphasis on risk-based and proportionality considerations should allow the Opinion to be adaptable over time, but indeed EIOPA will continue monitoring market developments and provide further guidance, where relevant.
18	Finance Watch	The use of AI in the insurance sector undeniably brings with it efficiency gains and cost-reductions for firms and speedier sales processes for consumers. However, it also entails major consumer risks that need to be properly mitigated by appropriate and robust regulation. A key risk in the insurance sector is that the use of AI by insurers to perform risk assessments and pricing risks leaving huge swathes of vulnerable consumers being denied insurance coverage or being faced with prohibitively high insurance premiums. Since its establishment, the insurance business model has been built on 'solidarity' or 'risk pooling' which has allowed potentially vulnerable consumers with higher risk profiles to still be able to afford insurance (be 'insurable') as the risk is spread out collectively across policyholders. The increasingly powerful algorithms of AI systems, however, enable highly granular risk assessments (highly personalized pricing) which endanger this business model. In addition, there is a risk of errors or biases in the AI model or in the data it relies on that can produce incorrect or discriminatory outcomes. In addition, the use of AI systems in the insurance sector also facilitates price optimisation practices, i.e. practices where, with the help of algorithmic tools, firms set prices that are not	Noted. EIOPA acknowledges that there are a great number of different uses of AI system in insurance. For this reason, and in line with the Impact Assessment, the Opinion focuses on providing high level guidance, and at a later stage EIOPA may provide more detailed guidance for specific uses of AI system in insurance, where relevant. The risks highlighted in this comment have been noted

		based on justified criteria such as the individual's level of risk with regards to insurance but on their price sensitivity (willingness to pay more). In the insurance sector, this can mean, for example, assessing whether consumers tend to switch general insurance products, such as home or motor insurance at renewal, or tend to hold them for long periods of time and are therefore unlikely to react to price rises and shop around. It can also mean determining someone's likelihood to pay more based on non-risk based factors such as income, level of studies, and type of device used to purchase the insurance (brand of smartphone, tablet, desktop computer, etc.), location, apps downloaded etc. (for example, see: https://www.eiopa.europa.eu/document/download/30f4502b-3fe9-4fad-b2a3-aa66ea41e863_en?filename=Artificial%20intelligence%20governance%20principles.pdf). Lastly, errors or biases in AI systems or the data they rely on can lead to the unfair denial of insurance claims or the compensation for a claim being lower than justified. There have been numerous examples of this in recent industry practice. The fatal shooting of UnitedHealthcare CEO Brian Thompson, for example, led to public scrutiny of insurers which reveals that major insurers in the US have used biased AI models that unfairly deny insurance claims. A lawsuit filed against UnitedHealth in 2023 claims that 90% of the recommendations of the algorithm used by the insurer for insurance claims, known as nH Predict, are reversed on judicial appeal. Moreover, US insurer Cigna has faced legal action over its use of a separate biased algorithm to unfairly reject insurance claims. A complaint against it alleges that the insurer relies heavily on the automated system, allowing claims to be denied without any review of individual patient files (see: https://www.hsgac.senate.gov/wp-content/uploads/2024.10.17-PSI-Majority-Staff-Report-on-Medicare-Advantage.pdf and https://qz.com/unitedhealthcare-humana-ai-lawsuits-1851715765).	and incorporated to the Impact Assessment.
19	Insurance and Pensions - Denmark	Modeling of risks is a core task in insurance, which is why the industry has extensive experience with governance related to models, including data, output validation, etc. Insurance and Pensions Denmark therefore support the purpose of the Opinion; namely to ensure that guidance is provided on the specific characteristics of AI models in order to ensure that companies can take these special characteristics into account and ensure that AI models meet the same requirements as other models used in the industry. This said, we also see a need for the Opinion to underline, that a model based on AI should not be subjected to additional requirements com-pared to other models used in the industry. This would also be in line with point 2.7 – stating that "This Opinion does not set out new	Noted. The Opinion does not create new requirements and does not alter the scope of insurance legislation mentioned therein. The Opinion does not establish a supervisory checklist, but rather it follows a holistic approach to AI governance and risk management anchored in risk-based and

		requirements". In addition to this, we consider it of outmost importance, that the Opin-ion does not go beyond existing regulations – and in doing this, we see a strong need to emphasize in the individual sections of the Opinion which requirements derive from which legislation, so that companies are not in doubt about the scope and which use cases are subject to which requirements. As stated in section 2.7, it is essential to ensure that the guidance does not impose new requirements. Therefore, it must be completely clear; if, where and when the guidance goes beyond existing legislation, these parts should be clearly marked as "purely inspirational". The final sentence in point 2.7 (inserted below) sets a relatively "strict" threshold that defines the entire document as representing the supervisory authorities' expectations. "2.7 […] This is achieved by setting high-level supervisory expectations of the governance and risk-management principles that supervisors expect undertakings to develop to ensure a responsible use of AI sys-tems, including by reflecting risk-based and proportionality considerations." If a given element is not covered by Solvency II and IDD (or other referenced legislation) it should be deleted or as a minimum be presented as supplementary measures or with similar wording that clearly indi-cates such elements are merely recommendations without legal basis and cannot be part of supervisory expectations. Doing this will add clarity. As a general comment, we see the current unclarity of scope for the different elements in the Opinion as an overarching challenge. Throughout the Opinion different sections first list legislative references i.e. IDD or Solvency II, which have very different legal scopes. Then the Opinion presents requirements formulated broadly as applica-ble for all AI-systems. In order to be in line with section 2.6 and 2.7 each section should clearly reference which requirements stem from which legislation, so that ap-plication scope is clear for companies. If the application scope is unclear, the Opinion risks 1) adding new re-quirements where not applicable (in contradiction to point 2.7) and 2) adding unclarity as to when sectorial	proportionality considerations. The Opinion clarifies that sectoral legislation requires adequate and proportionate governance and risk management measures when using mathematical models, regardless of whether they are considered AI systems or not. In this sense, it is not about additional requirements, but about adapting governance and risks management measures to address the specificities of AI systems. The references in the Opinion to articles from Solvency II, DORA, and IDD, which are not exhaustive, do not affect their scope of application. However, the principles outlined in the Opinion remain applicable to the use of AI systems in insurance.

		legislation will apply in practice. We therefore strongly suggest, that the Opinion clearly specifies the scope and legal basis for each suggested element. Doing this is crucial to achieve the overarching goal on providing clarity on the main princi-ples and requirements foreseen in insurance sectoral legislation (point 2.6). In addition, a short explanation on the scope of the referenced legisla-tion (mainly IDD, Solvency II and DORA) could in addition be useful to have included in the Opinion.	
20	Wind Tre S.p.A.	In responding to this Consultation Paper we believe is important to underline, as also referred to by EIOPA at recital 2.3, as AI Act applies to all sectors of the economy and aims at ensuring a high level of protection for fundamental rights, health, and safety. Moreover AI Act identifies as high-risk the use of AI systems for risk assessment and pricing in relation to natural persons in the case of life and health insurance. The AI Act has clearly distinguished the responsibilities and obligations of providers and deployers of AI systems and general-purpose AI models: companies in the financial sector will generally be deployers and not providers.	Noted. The scope of the Opinion covers AI systems used in insurance that are not considered prohibited AI practices or high-risk under the AI Act, in order to avoid creating unnecessary overlaps and regulatory burdens.
21	Insur.Cap	We need XAI = explainable agentic insurance observability tool for tracing AI	Noted.
22	BEUC - The European Consumer Organisation	BEUC welcomes EIOPA's Opinion on AI Governance and risk management for insurances not falling under the high-risk categorisation. For consumers, every AI system can bring notable risks. In the insurance sector, risks include: o Unfair pricing and underwriting which can result from the use of irrelevant data (e.g. risk that an AI system establishes a price or a decision to offer an insurance contract or not on a random correlation instead of a well-explained causality) or poor data quality (e.g. if AI system learned decision-making with outdated medical data on the treatment of chronic diseases, the system will raise the price for a concerned consumer unfairly or unduly refuse to offer an insurance contract). o Undue refusals of claims due to poor assessment by the AI system (e.g. wrong interpretation of documents/images shared by the consumer) o Poor customer service based on chat bots/automated replies which do not provide the relevant or even false information	Noted. Some of the risks highlighted in this comment have been noted and incorporated to the Impact Assessment.
		Q2 - Do you have any comments on the scope of the Opinion?	

23	Mirko Kraft	It is acknowledged that EIOPA has chosen to focus in its opinion on AI systems that are neither prohibited nor classified as “high risk” under the AI Act. In the EIOPA opinion sect. 2.8 should be updated: The European Commission published guidelines on AI system definition (see https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application). Reference should be made also to the Commission’s guidelines on prohibited artificial intelligence (AI) practices (see https://digital-strategy.ec.europa.eu/en/library/ commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act).	Noted. The Opinion now also includes an explicit reference to the Commission’s Guidelines on AI system definition where linear and logistic regression are referenced. EIOPA acknowledges that further guidance may be provided in the future in this regard.
24	BIPAR	BIPAR notes that “the Opinion does not set out new requirements (…) but rather provides guidance on how different provisions of insurance sectorial legislation should be interpreted in the context of AI systems which did not exist or were not widely used at the time the legislation was approved”. EIOPA continues by explaining that “ this is achieved by setting high-level supervisory expectations of the governance and risk management principles that supervisors expect undertakings to develop to ensure a responsible use of AI systems, including by reflecting risk-based and proportionality considerations”. BIPAR underlines the importance of having a proportionality approach in the entire Opinion, particular when the Opinion covers – very limited- the activities of intermediaries, the latter being mostly micros and SMEs. BIPAR welcomes EIOPA objective not to impose new mandatory requirements, considering that the existing EU framework – Solvency II, IDD, GDPR, DORA, and now the AI Act itself – already constitutes a comprehensive and robust regime. Introducing additional detailed requirements would be beyond EIOPA remit and would risk overlapping or contradicting existing rules, creating legal confusion. BIPAR believes that the Opinion’s use of prescriptive language (particularly the term “should”) could contradict the Opinion’s objective and result in new supervisory expectations for undertakings to meet. Recommendation rather than obligation are more appropriate in this context. Therefore, BIPAR suggests amending the language of the Opinion so that it is in line with its stated objectives and does not introduce new obligations in addition to those currently applicable.	Noted. The Opinion does not create new requirements and does not alter the scope of insurance legislation mentioned therein. The Opinion does not establish a supervisory checklist, but rather it follows a holistic approach to AI governance and risk management anchored in risk-based and proportionality considerations. The references in the Opinion to articles from Solvency II, DORA, and IDD, which are not exhaustive, do not affect their scope of application. However, the principles outlined in the Opinion remain applicable to the use of AI systems in insurance, following a risk-

			based and proportionate approach.
25	Studio legale Floreani	The delineation of the Opinion's scope would benefit from further refinement to ensure alignment with the principle of proportionality and with the differentiated roles of insurance undertakings and insurance distributors, as outlined in Directive (EU) 2016/97 (IDD). A clear allocation of responsibilities is particularly important in relation to the adoption and oversight of artificial intelligence (AI) systems, the management of related operational and conduct risks, and compliance obligations under applicable regulatory frameworks. The Opinion should further differentiate among categories of distributors – including tied agents, multi-mandate intermediaries, and bancassurance operators – ensuring the applicability of requirements is proportionate to their operational complexity and business model. Moreover, AI-driven processes that affect the pre-contractual phase, client interaction, and consent mechanisms under the General Data Protection Regulation (GDPR) require precise clarification within the scope. It is therefore recommended that: Distinct supervisory expectations be defined for insurance undertakings and insurance distributors. Sector-specific templates or adapted pre-contractual disclosures be developed for clients, especially in the context of automated processes.	Noted. In line with the Opinion's Impact Assessment, EIOPA will focus on providing high-level guidance. This approach is complemented by specific examples included in the Annex, which are not intended to be considered prescriptive guidance but rather illustrate possible practical ways to implement some of the high-level principles included in the Opinion. Moreover, based on the AI governance framework proposed in the Opinion, EIOPA envisages subsequently developing more detailed analysis on specific AI systems or issues arising from the use of AI systems in insurance and providing further guidance, as relevant
26	AFPA, Austrian Financial & Insurance Professionals Association	Der eingeschränkte Umfang auf nicht-hochriskante KI ist sinnvoll. Wichtig sind eine klare Abgrenzung und Vermeidung von Grauzonen. Einheitliche Regeln sind unabdingbar um den Binnenmarkt zu stärken. The limited scope to non-high-risk AI is sensible. Clear delineation and avoidance of gray areas are important. Uniform rules are indispensable to strengthen the internal market.	Noted.
28	Insurance Europe	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	Noted. The Opinion clarifies that it does not set out new requirements and in particular it does not

		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”).	seek to alter the scope of the AI Act by extending the requirements of the AI Act for high-risk AI systems to all AI systems used in insurance. It also does not alter the scope of application of the sectoral legislation mentioned therein. The Opinion provides guidance on how to interpret various provisions of the existing insurance sectoral legislation in the context of AI systems. The references in the Opinion to articles from Solvency II, DORA, and IDD, which are not exhaustive, do not affect their scope of application. However, the principles outlined in the Opinion remain applicable to the use of AI systems in insurance, following a risk-based and proportionate approach.
30	Lloyd’s Market Association	We note that High Risk AI use cases are not in scope for this Opinion. However, we believe that Annex 1, as currently drafted, could result in de facto standards being applied where these are not necessarily appropriate, notwithstanding the fact that at least part of Annex 1 only refers to High Risk AI Use Cases, which is not within the scope of this report. We therefore recommend either (i) referring only to the underlying AI Governance Principles Report in the body of the Opinion, or (ii) adding wording to Annex 1 to clarify that the principles are offered as illustrative guidance, intended to inform thinking rather than prescribe solutions for every use case.	Noted. Further wording has been added to the Annex to clarify that the examples included therein have been included for illustrative purposes only and are not intended to be considered as prescriptive guidance.

31	European Federation of Financial Advisers and Financial Intermediaries (FECIF)	FECIF believes that, in addressing the subject matter of the Opinion under consultation, the social security component should also be taken into account.	Noted. Social security systems are not included in EIOPA's mandate and therefore they not referred to in the Opinion.
32	AMICE	We support EIOPA's choice of limiting the scope of the Opinion to AI systems that are not classified as high-risk or prohibited under the AI Act, as this approach limits the risk of duplicative requirements. However, from this perspective, considering the undergoing work of the European Commission on potential new Guidelines for AI in financial services, we invite EIOPA to ensure maximum coordination with the other competent policymakers before publishing its Opinion, in order to avoid the introduction of conflicting or redundant regulatory frameworks.	Noted. EIOPA recognises the value of collaborating with the European Commission's AI Office and other relevant authorities to ensure a coordinated approach, avoid duplication of efforts, and prevent unnecessary regulatory burdens. This collaborative approach is already being implemented by EIOPA and is expected to continue in the future.
33	Institute of International Finance	We appreciate the recognition that 'Limited derogations are introduced to address overlaps with existing sectorial insurance legislation' (para 2.4), though these could be more clearly articulated in this Opinion: our members have consistently raised with us concerns about overlaps among the various parts of the EU digital finance acquis including the interfaces between the EU AI Act and other legislation. We welcome that the Opinion 'does not cover prohibited AI practices or high-risk AI systems under the AI Act' (para 2.6), which appropriately limits its scope and avoids regulatory overlap. For this reason, as noted below, we suggest that the material put forward in Annex I relating to "high-risk AI use cases" may not belong in the Opinion. Should EIOPA proceed with retaining this content, then the critical distinction between a high-risk AI system (as defined in the AI Act) and a high-risk use case must be precisely articulated and thoroughly explained with explicit reference to the established legal framework and concepts in the AI Act. The scope should more clearly distinguish between customer-facing use cases and internal use cases, with proportionately different requirements. Supervisory attention should also focus on newer applications of AI (such as generative AI (GenAI)) in insurance practices and	Noted. EIOPA recognises the value of collaborating with the European Commission's AI Office and other relevant authorities to ensure a coordinated approach, avoid duplication of efforts, and prevent unnecessary regulatory burdens. This collaborative approach is already being implemented by EIOPA and is expected to continue in the future. The scope of the Opinion covers AI systems used in insurance that are not

		where the use of AI materially impacts consumers or could materially impact insurer solvency, rather than “classical” actuarial models and similar systems. While GenAI at scale is a relatively emerging technology, supervisors should avoid adding to or exacerbating hyperbole around AI. AI and ML systems in the insurance sector have been deployed in production for some time, and are already subject to existing regulatory and risk management frameworks. Analytical systems are used in claims fraud detection and claims processing, underwriting risk scoring, and streamlining customer servicing, and are subject to existing enterprise-wide risk management frameworks. We would consequently recommend narrowing the discussion on AI to focus on generative AI and deep neural networks, characterized by: greater capability for autonomous learning and adaptation; complex inferential capabilities beyond traditional statistical methods. This would exclude well-established methods that have been subject to existing risk management frameworks for considerable time, such as: Linear/logistic regression; Decision trees and random forests; Rule-based expert systems; and traditional statistical and predictive modeling. As to the legal basis, our members are concerned that in some areas, including data governance and transparency, EIOPA appears to be straying outside the subject-matter that is properly within its legal mandate. We would ask that EIOPA carefully examine its proposed guidance for true relevance to those legislative acts that are cited as forming the legal basis (namely the Solvency II Directive, Insurance Distribution Directive (IDD), Digital Operational Resilience Act and certain subordinate legislative acts).	considered prohibited AI practices or high-risk under the AI Act. However, undertakings can adapt the governance and risk management to the specificities of different AI systems used in insurance, taking into account risk-based and proportionality considerations. The references in the Opinion to articles from Solvency II, DORA, and IDD, which are not exhaustive, do not affect their scope of application. However, the principles outlined in the Opinion remain applicable to the use of AI systems in insurance, following a risk-based and proportionate approach.
34	Gesamtverband der Deutschen Versicherungswirtschaft	See Q1.	Noted.
35	CNP Assurances	The scope of the opinion is not clearly defined, particularly regarding whether the intention is to apply the AI Act's risk management system for high-risk AI systems to all AI-based use cases employed by insurance companies, or only to use cases that fall within the scope of the three regulations on which the opinion is based (IDD, Solvency II, DORA). Clarification on the use cases of AI, whether "limited" or "high impact," should be provided to justify more in-depth examinations. Additionally, the application of the opinion to different industry branches, as well as comments on generative AI and third-party models, should be	Noted. The Opinion clarifies that it does not set out new requirements and in particular it does not seek to alter the scope of the AI Act by extending the requirements of the AI Act for high-risk AI systems to

		clarified to enable a better risk management approach. AI use cases should be identified based on the full value chain, enabling quick impact assessments for low-risk AI systems and leading to their classification.	all AI systems used in insurance. The Opinion provides guidance on how to interpret various provisions of the existing insurance sectoral legislation in the context of AI systems. The references in the Opinion to articles from Solvency II, DORA, and IDD, which are not exhaustive, do not affect their scope of application. However, the principles outlined in the Opinion remain applicable to the use of AI systems in insurance, following a risk-based and proportionate approach. Moreover, the Opinion includes some examples of criteria that undertakings should take into account when assessing the impact of uses of AI systems, but it does not provide a prescriptive delineation in line with the principle-based approach of the Opinion. Furthermore, it has also been clarified that the impact assessment should be limited in cases where AI systems are

			expected to have a limited impact.
36	IRSG	We appreciate that EIOPA has chosen to focus its Opinion on AI systems that are neither prohibited nor classified as “high risk” under the AI Act. This narrow scope acknowledges that the most sensitive AI applications are already subject to extensive supervisory frameworks, thus avoiding the risks of duplicative requirements. Nevertheless, we would like to note that recent stakeholder consultation by the European Commission regarding guidance for AI in financial services sector suggests that additional regulations may soon emerge. If separate bodies issue overlapping requirements, the result could be a fragmented and incoherent regulatory framework that would weaken rule of law while complicating compliance. Thus, we encourage EIOPA to coordinate closely with the European Commission and other relevant authorities. We recommend that EIOPA considers withholding the publication of its Opinion until the European Commission has either published or decided not to publish its guidance on AI in financial services. This would ensure an harmonised and effective framework, limiting the risks of duplicative or conflicting requirements. Sect. 2.8 should be updated: The European Commission published guidelines on AI system definition (see https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application). Reference should be made also to the Commission’s guidelines on prohibited artificial intelligence (AI) practices (see https://digital-strategy.ec.europa.eu/en/library/ commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act).	Noted. EIOPA recognises the value of collaborating with the European Commission's AI Office and other relevant authorities to ensure a coordinated approach, avoid duplication of efforts, and prevent unnecessary regulatory burdens. This collaborative approach is already being implemented by EIOPA and is expected to continue in the future. The Opinion now also includes an explicit reference to the Commission’s Guidelines on AI system definition where linear and logistic regression are referenced. EIOPA acknowledges that further guidance may be provided in the future in this regard.
37	CRO Forum	The CRO Forum understands and welcomes that the Opinion is limited to AI use cases that fall within the scope of application of the Solvency II Directive, the Insurance Distribution Directive or the Digital Operational Resilience Act and that are not considered to be high-risk according to the AI Act. Thus, any other AI use cases would not be in the scope of the Opinion. However, for the sake of legal certainty, confirmation on this part would be appreciated. We are supportive that the Opinion does not apply to high-risk AI use cases. But this is contradicted in section 3.23 which refers to Annex I where there are examples of recordkeeping for ‘high-risk AI use cases‘. This contradicts the statement that the Opinion	Noted. The scope of the Opinion covers AI systems used in insurance that are not considered prohibited AI practices or high-risk under the AI Act. The consideration of high-risk AI systems in the AI Act has its own meaning

		does not apply to high-risk AI. The CRO Forum supports the EIOPA assertion (in section 2.7) that the Opinion should not set out new requirements or extend the requirements of the EU AI Act, focusing rather on advice, illustrations, and recommendations for good practices, reflecting risk based and proportionality considerations. However, the frequent use of 'should' through the Opinion does contradict the assertion that the Opinion does not set out requirements. A feedback loop mechanism could be established, so that insurers can report back to EIOPA on the practical challenges faced during the implementation of the Opinion, allowing for continuous improvement.	and legal implications, which are independent of the outcome of the impact assessment foreseen in the Opinion. Further wording has been added to the Annex to clarify that the examples included therein have been included for illustrative purposes only and are not intended to be considered as prescriptive guidance. The Opinion also clarified that is does not create new requirements and does not alter the scope of insurance legislation mentioned therein. The use of terminology such as "should" is common in similar guidance documents developed by EIOPA in the past. EIOPA will indeed continue monitoring market developments in close cooperation with stakeholders and provide further guidance, where relevant.
38	European Financial Congress	The scope of the opinion covers only AI systems in insurance that are not prohibited or deemed high-risk under the AI Act. This approach reduces the risk of overlapping requirements, but in practice means that even low-risk systems are subject to detailed interpretation of sector regulations.	Noted. A reference to the need to follow a risk-based and proportionate approach has now been

		The lack of explicit exemptions for small entities or minimal risk applications can lead to excessive caution and cost, especially since the Opinion suggests implementing policies, training and documentation in these cases as well. It is worth advocating for clarification of the scope by clearly indicating when and to what extent the requirements can be limited or simplified.	clearly included at the beginning of each principle outlined in the Opinion. EIOPA has also clarified that the supervisory expectations for low-risk AI systems will be very limited. Furthermore, it has also been clarified that the impact assessment should be limited in cases where AI systems are expected to have a limited impact.
39	European Confederation of Institutes of Internal Auditing	Solvency II and other model requirements would fall under the OECD AI definition and not under the AI Act definition, we wonder how to manage this discrepancy. - Considering the rapid advancements in AI technology since the introduction of the EU AI Act, we wonder if EIOPA should not include any perspective on AI Agents or other developments in AI.	Noted. EIOPA has retained the definition of AI systems of the AI Act, to ensure a consistency with the approach followed in the European Union. The principles-based nature of the Opinion and its emphasis on risk-based and proportionality considerations should allow the Opinion to be adaptable over time, but indeed EIOPA will continue monitoring market developments and provide further guidance, where relevant.
40	BETTER FINANCE	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	Noted. The Opinion states that its scope covers AI systems used in insurance that are not considered prohibited AI practices or high-risk under the AI Act.

		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.	
41	Actuarial Association of Europe	Key message: The AAE supports the scope of the Opinion, focusing on non-high-risk AI systems, and recognises the importance of aligning with the AI Act. However, it would be helpful for EIOPA to provide greater clarity on borderline or potentially high-impact use cases that may merit enhanced scrutiny. In addition, a clearer articulation of how the Opinion applies across different parts of the insurance sector, along with observations on Generative AI and third-party models, could support consistent and practical application of risk management practices. Detailed response: We agree with the principle-based scope of the Opinion, which appropriately focuses on AI systems not classified as high-risk under the AI Act, and allows for flexibility to reflect the specific business models and products used across the European insurance sector. The Opinion rightly reflects the AI Act's designation of life and health underwriting as high-risk. However, further clarity would be helpful for borderline insurance use cases that may not meet the formal high-risk definition but could still have material impacts on individuals. For instance, AI used in motor or home insurance might affect access to essential services, and systems involved in non-life claims settlement may have life-altering financial consequences. Guidance on whether such cases warrant enhanced governance, or how they relate to the overall risk-based approach, would support consistent interpretation across the sector. We suggest EIOPA could provide more detail on how the Opinion applies across various insurance product lines, recognising that the risk profile of AI applications may differ substantially between, for example, personal lines and commercial or reinsurance business. This would help undertakings assess proportionality more accurately. Additionally, we propose that EIOPA may wish to briefly reflect on emerging issues such as Generative AI (GenAI), especially in claims fraud detection where synthetic content generation presents new challenges. Similarly, acknowledging the differing governance needs of AI systems developed in-house versus those sourced externally — including open-source solutions — may assist undertakings in tailoring controls appropriately. These considerations could be explored further in future iterations or complementary workstreams.	Noted. The Opinion acknowledges that it does not seek to extend the requirements for high-risk AI systems of the AI Act to all uses of AI systems in insurance, and that there are varying levels of risk among AI systems that are not prohibited or considered high-risk under the AI Act. The consideration of high-risk AI systems in the AI Act has its own meaning and legal implications, which are independent of the outcome of the impact assessment foreseen in the Opinion. The Opinion includes some examples of criteria that undertakings should take into account when assessing the impact of uses of AI systems, but it does not provide a prescriptive delineation of higher and lower risk uses of AI systems, in line with the principle-based approach of the Opinion.

		To improve clarity and usability, we suggest EIOPA include several explicit examples of in-scope AI systems within the introduction or annex. This could include more complex applications such as forecasting, weather or catastrophe modelling, and advanced actuarial risk assessment, particularly where deep learning or neural networks are involved. Such examples would help ground the Opinion in real-world use cases and address concerns that the scope may appear too abstract.	The Opinion also now includes more detailed guidance on how to address the issues arising from the use of third-party AI systems, which is often the case of Generative AI systems.
42	Finance Watch	Given the significant risks to consumers outlined in our answer to Q1, we are of the view that the chosen approach to only issue high-level guidance is not sufficient to adequately protect consumers from the considerable risks stemming from the use of AI in the insurance sector. At a minimum there would be a need for detailed guidance - and preferably even going beyond this and making legislative changes to the relevant sectoral insurance legislation (IDD, Solvency II) so that the measures are legally-binding. In addition, in our view, there is a need to extend the scope of high-risk AI systems in the AI Act by broadening the scope of Annex III of the AI Act to cover all insurance products via adoption of delegated acts as per Article 7 of the AI Act. Not classifying the application of AI in the provision of all retail insurance products as high-risk makes the EU AI Act inconsistent with its goal to prevent AI systems from posing a risk to consumer access to essential private services and benefits. The unfair denial of essential financial services, which includes all insurance products and bank accounts, entails significant negative impacts on the economic and life prospects of a person. Not having access to essential insurance products can lead to financial ruin of a citizen if they are not insured against unexpected events such as accidents, the loss of employment or damages to their home (and in some Member States, having home insurance is a requirement to be able to rent an apartment). Annex III (5) of the EU AI Act states that AI systems associated with the access to and enjoyment of essential private services and benefits should be classified as high-risk. It correctly includes 1. AI systems intended to be used to evaluate the creditworthiness of natural persons and 2. AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance under this category. However, the regulation is inconsistent in that it does not include the risk assessment and pricing of other insurance products and customer risk assessments when opening a bank account under this category as well.	Noted. In line with the Opinion's Impact Assessment, EIOPA will focus on providing high-level guidance. This approach is complemented by specific examples included in the Annex, which are not intended to be considered prescriptive guidance but rather illustrate possible practical ways to implement some of the high-level principles included in the Opinion. Moreover, based on the AI governance framework proposed in the Opinion, EIOPA envisages subsequently developing more detailed analysis on specific AI systems or issues arising from the use of AI systems in insurance and providing further guidance, as relevant Moreover, EIOPA is not competent to amend the list of high-risk AI systems

			of the AI Act, but we will collaborate with the European Commission and the market surveillance authorities in the implementation of the AI Act.
43	Insurance and Pensions - Denmark	We find the elements covered in the Opinion relevant and that we think that the concrete actions are balanced correctly to achieve the overall goal of setting high-level guidelines – and still leaving room for the companies to adjust to their specific business practices. Overall, we consider the Opinion to be a well-structured and thoughtful contribution to AI governance and risk management in the industry. In terms of clarity we feel, that the Opinion will – in addition to clarity on legal basis - benefit from further underlining the areas of proportion-ality in scope and the importance of a risk-based approach. Insurance and Pensions Denmark therefore suggest, that 1) the princi-ple of proportionality it is more clearly emphasized, making it stand out as an indispensable overarching basis for all measures, and 2) That the principle of proportionality could be reiterated in relation to the specific points in the follow sections - especially in areas where the text ap-proaches the limits of Solvency II and IDD. We also see it as important the Opinion mentions and recognizes, that Solvency II and IDD have different approaches to proportionality: Solv 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 insur-ance product. In relation to this we recognize that a risk based and proportionate ap-proach was repeated several times as a defining foundation for the Opinion by EIOPA during the webinar on April 7th. We agree with the emphasis on these points during the webinar, stating that insurers should:	Noted. A reference to the need to follow a risk-based and proportionate approach has now been clearly included at the beginning of each principle outlined in the Opinion. EIOPA has also clarified that the supervisory expectations for low-risk AI systems will be very limited. Furthermore, it has also been clarified that the impact assessment should be limited in cases where AI systems are expected to have a limited impact. The Opinion has clarified that references to sectoral legislation do not alter the scope of application to the insurance sector legislation mentioned therein. However, the principles laid out in the Opinion, including the need to take into account risk-based and proportionality considerations, remain

		1) Assess the risk on different AI use cases 2) Deploy proportionate measures (According to relevant regulation – and beyond that purely voluntary, but still relevant) The proportionality and risk considerations are central in order to bal-ance concrete actions with risk to avoid unnecessary burdens. The importance of a risk-based approach was also underlined during the webinar – and it was underlines that the specific actions in the Opinion was to be used (or not used) based on risk and proportionality. (low risk = low actions / high risk = more actions) We therefore suggest, that in addition to proportionality the risk based approach should be further clarified in the beginning – as an overarch-ing element - as these considerations inform all other measures in the Opinion.	applicable to the use of AI systems in insurance.
44	Wind Tre S.p.A.	Therefore we retain that: this Consultation Paper is an excellent opportunity to detail the provisions of the AI Act in the insurance sector without changing an already outlined framework with regard to risk levels; in formulating undertakings that apply to the insurance market, it will be necessary to evaluate to pay close attention to the fact that obligations that the AI Act has attributed to providers are not replicated or overlapped with financial institutions that will be deployers and not providers principles that underlie the obligations imposed by the AI Act on high-risk systems cannot be replicated on systems of other types and purposes.	Noted. The scope of the Opinion covers AI systems used in insurance that are not considered prohibited AI practices or high-risk under the AI Act, in order to avoid creating unnecessary overlaps and regulatory burdens. The Opinion also now includes more detailed guidance on how to address the issues arising from the use of third-party AI systems. The Opinion is based on insurance sector legislation and follows a principle-based approach, and it is in line with the underlying

			principles and requirements of the AI Act and other international initiatives in this area.
45	ANASF	We believe that in addressing the subject matter of the Opinion under consultation, the social security component should also be taken into account.	Noted. Social security systems are not included in EIOPA's mandate and therefore they not referred in the Opinion.
46	BEUC - The European Consumer Organisation	- BEUC welcomes the Opinion to provide guidance on how different provisions of insurance sectorial legislation should be interpreted in the context of AI systems. - In addition, BEUC recommends EIOPA to investigate whether further types of insurances should be classified as high-risk. From a consumer perspective, the list of high-risk insurances is very limited, and we observe high-risk AI practices also for other types of insurances (e.g. home insurance and motor insurance) which are currently not listed as such. - BEUC recommends reformulating point 2.5 which foresees that AI systems outside the high-risk category will operate "without new requirements" as it gives the impression that insurance operators do not have to take any or only very limited (e.g. transparency) measures for such AI systems. We would recommend formulating as follows: "The remaining AI systems in insurance that are not prohibited AI practices and that are not considered to be high-risk continue to operate subject to existing legislation, including sectorial legislation. In addition, Articles 6(3), 6(4) and 7 of the AI Act apply. - BEUC recommends emphasising that the guidelines apply to all insurance undertakings and distributors and technical service providers to which the development or operation of AI systems has been outsourced. Insurance distributors include for instance also comparison websites.	Noted. EIOPA is not competent to amend the list of high-risk AI systems of the AI Act, but we will collaborate with the European Commission and the market surveillance authorities in the implementation of the AI Act. The Opinion does not set out new requirements; it provides guidance on how to interpret various provisions of the existing insurance sectoral legislation. The Opinion also now includes more detailed guidance on how to address the issues arising from the use of third-party AI systems, in particular by acknowledging the importance of the collaboration between

			undertakings and third-party service providers to address the risks arising from AI systems in insurance.
47	AI & Partners	The scope appropriately excludes prohibited and high-risk AI applications covered under the AI Act, focusing instead on ensuring responsible governance for lower-risk systems. However, more detailed guidance on the practical implementation of proportionality in AI governance would be helpful, particularly for mid-tier insurers. Additionally, further clarification on how this Opinion interacts with existing GDPR and Solvency II requirements could prevent regulatory fragmentation. Expanding on best practices for voluntary codes of conduct and AI literacy initiatives would also help insurers develop more effective governance frameworks tailored to their specific operational risks.	Noted. In line with the Opinion's Impact Assessment, EIOPA has focused on providing high-level guidance. This approach is complemented by specific examples included in the Annex, which are not intended to be considered prescriptive guidance, EIOPA envisages subsequently developing more detailed analysis on specific AI systems or issues arising from the use of AI systems in insurance and providing further guidance, as relevant. The Opinion focuses on the main provisions in insurance sectorial legislation within EIOPA's remit that are relevant to the use of AI systems, but it is acknowledged that other legislations such the GDPR may also include provisions relevant to the use of AI systems.

		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?	
48	BIPAR	Generally speaking, we find the risk-based approach proposed sensible, and the assessment proposed in Annex I helpful. We would like to stress the importance of also assessing the impact of large scale use of emerging technologies on the competitive landscape. Although the examples and categories of risks EIOPA mentions in this section of the Opinion are not limitative, they refer mainly to the risks of the entity itself and consumers entering into contact with that entity. We believe that it would be useful to also assess the impact on the overall market. Large scale technologies can lead to oligopolistic outcomes and, if we add the regulatory constraints in the financial sector, these risks become even more relevant. Therefore, we believe a specific paragraph in the Opinion should refer to risks of adverse effects on the level of competition within a national or even the European market. A specific example is that the proportionality approach should also mean that smaller players could apply lighter rules until certain levels of impact are reached. Another example is situations where insurers have several distribution channels. In case such an insurer would choose to offer various AI services to the clients they have in common with various intermediaries and would choose to limit by design the access of the intermediary to the AI-based facilities, this could lead to the creation of an unfair competitive advantage for the large-scale player. A solution for preventing these kind of effects is that undertakings are mandated to make available by design integration tools to intermediaries (such as API's) for any AI based solution regarding common customers interactions. Another "reflection" in this respect may also be that AI based models for claims handling, pricing or risk assessment remain challengeable by human intermediaries, in order for them to be able to service and advice their clients properly when dealing with AI-based systems. It could also be further clarified if the risk of developing AI tooling in house carries different risk levels. It is important that standards/protocols for communication methods to end customers are	Noted. The Opinion follows a risk-based and proportionate approach, which should limit the impact on smaller undertakings. The Opinion has further emphasized the need to follow a risk-based and proportionate approach under each of the principles outlined in the Opinion. The Opinion also now includes states under the transparency and explainability principle that, where relevant, insurance intermediaries should also be informed by insurance undertakings when a decision is made on the basis of an AI systems so that they can comply with their legal obligations before the customer. The Opinion also now includes more detailed guidance on how to address the issues arising from the use of third-party AI systems, in particular by

		clearly defined, according to the different AI models adopted by manufacturers in the various areas of use. Distributors should be informed through adequate information flows on the models adopted by manufacturers to ensure compliance with situations described in point 3.27 of the Opinion for example (see also below, response to question 8). We start from the assumption that every product that comes on the market went through the POG process (AI or no AI). Intermediaries must be able to rely on the product POG process and the disclosures made by the manufacturers (see Article 25.1 IDD)	acknowledging the importance of the collaboration between undertakings and third-party service providers to address the risks arising from AI systems in insurance.
49	Studio legale Floreani	The current governance approach, while aligned with overarching risk-based principles, appears overly general and insufficiently adapted to the structural differences between insurance undertakings and distributors. A more granular articulation of obligations is required, particularly in the assessment of ICT-related risks as prescribed under Regulation (EU) 2022/2554 (DORA). In the distribution context, risk exposure may vary significantly depending on the nature and scale of the intermediary's activities. Accordingly, it is suggested to: Clearly delineate responsibilities for preventing unauthorised system manipulation or misuse. Define proportionate technical and organisational security measures applicable to distribution channels. Establish harmonised incident response procedures for AI-related anomalies. Introduce a tiered risk classification framework and develop operational guidance tailored to insurance intermediaries.	Noted. In line with the Impact Assessment, the Opinion focuses on providing high level guidance, also in relation to ICT related risks (covered under the accuracy, robustness and cybersecurity principle). At a later stage EIOPA may provide more detailed guidance for specific uses of AI system in insurance, where relevant. The same approach is followed with regards to the impact assessment; the Opinion includes some examples of criteria that undertakings should take into account when assessing the impact of uses of AI systems, but it does not provide a prescriptive delineation of higher and lower risk uses of AI systems, in line with

			the principle-based approach of the Opinion. This approach is complemented by specific examples included in the Annex, which are not intended to be considered prescriptive guidance.
50	AFPA, Austrian Financial & Insurance Professionals Association	Ein risikobasierter, verhältnismäßiger Ansatz ist essenziell. Anforderungen müssen je nach Risiko- und Unternehmensgröße skaliert werden, um Innovation nicht im Keim zu ersticken. Folge wäre ansonsten ein weiterer Rückfall der europäischen Wirtschaft im internationalen Vergleich. Als große Herausforderung für die Unternehmen ist anzumerken, dass neben dem AI-Act auch DORA als bereits beschlossenes Regularium neu zu den bestehenden Regelungen aufgenommen wird. Weiters ist an dieser Stelle unbedingt der Vorschlag über einen Rahmen für den Zugang zu Finanzdaten (FIDA) zu erwähnen. In all diesen Bereichen gibt es aktuell noch unzählige Fragen zu einer einheitlichen Beurteilung und Kontrolltätigkeit. Die Unternehmen sind hier durch einen massiven Umbruch enorm gefordert. Einerseits mussten bzw. müssen zahlreiche neue Vorgaben intern aufbereitet und in die eigene Prozessstruktur integriert werden, andererseits wirft das Spektrum der KI-Systeme generell noch unzählige Strukturfragen auf. Hier wird besonders auf das Problem der Abhängigkeit von US-Tools hingewiesen. Erfahrungsgemäß erfolgt hier die proaktive Mitwirkung der US-Anbieter äußerst zurückhaltend und schleppend. Und zunehmend mit der Größe des Anbieters und deren unbestreitbarer Marktbeherrschung, wird den Nutzern ein häufig unlösbares Problem aufgebürdet. Zwischen Anbieter und Nutzer herrscht nicht annähernde „Waffengleichheit“. Bei diesem Punkt ist als besondere Herausforderung die geplante FIDA-Verordnung zu erwähnen. Wenn, wie zu erwarten, der Datenaustausch und eine Datenanalyse unter enger Einbindung von KI-Tools erfolgen wird, würde Europa durch die Marktbeherrschung der US-Tools und US-Speicherzentren die Datenhoheit in einer noch höheren Intensität verlieren. Hier sind eine proaktive Mitwirkung und Unterstützung der europäischen Aufsichtsbehörden unabdingbar. Aus unserer Sicht sind die KI-Anbieter noch intensiver an die EU-Regularien zu binden, beispielsweise durch eine verpflichtende Betriebsstätte in Europa. Dadurch werden aufsichtsrechtliche Prüfmöglichkeiten verbessert bzw. erst realistisch ermöglicht. A risk-based, proportional approach is essential. Requirements must be scaled according to risk and company size to avoid stifling innovation. Otherwise, the European economy would	Noted. The Opinion follows a risk-based and proportionate approach, which should limit the impact on smaller undertakings. The Opinion has further emphasized the need to follow a risk-based and proportionate approach under each of the principles outlined in the Opinion. The Opinion also now includes more detailed guidance on how to address the issues arising from the use of third-party AI systems, in particular by acknowledging the importance of the collaboration between undertakings and third-party service providers to address the risks arising from AI systems in insurance. The Opinion does not explicitly mention the

		fall further behind in international comparison. A major challenge for companies is that, in addition to the AI Act, DORA, as an already adopted regulation, is being added to the existing regulations. Furthermore, the proposal for a framework for access to financial data (FIDA) must be mentioned here. In all these areas, there are currently countless questions regarding uniform assessment and control activities. Companies are enormously challenged by this massive upheaval. On the one hand, numerous new requirements had to be or must be processed internally and integrated into their own process structure. On the other hand, the spectrum of AI systems generally raises countless structural questions. Here, the problem of dependence on US tools is particularly highlighted. Experience shows that the proactive involvement of US providers is extremely hesitant and slow. And increasingly, with the size of the provider and their undeniable market dominance, users are burdened with a frequently unsolvable problem. There is no "level playing field" between providers and users. The planned FIDA regulation is a particular challenge in this regard. If, as expected, data exchange and data analysis are to take place with close integration of AI tools, Europe would lose data sovereignty to an even greater extent due to the market dominance of US tools and US data centers. Proactive involvement and support from European supervisory authorities are indispensable here. In our view, AI providers must be more closely bound to EU regulations, for example, through a mandatory establishment in Europe. This would improve or realistically enable supervisory audit possibilities.	proposal for a framework for access to financial data (FIDA) given that the legislative process is still on-going and its final outcome is uncertain.
52	Insurance Europe	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	Noted. The Opinion follows a risk-based and proportionate approach, which should limit the impact on smaller undertakings. The Opinion has further emphasized the need to follow a risk-based and proportionate approach under each of the principles outlined in the Opinion. In addition, while not providing an exhaustive list, the Opinion now includes further examples of the criteria that could be included in the impact

		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 [...]."	assessment, such as the differentiation between internal uses and consumer-facing applications, or the number of retail customers affected. Further examples are also included in the Annex. The Opinion has clarified that references to sectoral legislation do not alter the scope of application of the insurance sector legislation mentioned therein. However, the principles laid out in the Opinion, including the need to take into account risk-based and proportionality considerations, remain applicable to the use of AI systems in insurance. The term "responsible use" has been retained given that it is a widely recognized and established concept within the domain of AI governance, and it aligns with the principle-based approach of the Opinion.
54	Lloyd's Market Association	We agree that adopting a risk-based, proportionate approach calibrated to the level of risk is the appropriate measure. We also think the Opinion could benefit from a clearer distinction between AI usage which	Noted. While not providing an exhaustive list, the Opinion now includes further examples of the

		has a direct impact on customer outcomes, and usage which is purely internal, for instance, using AI to summarise a document for internal purposes. It should be made clear that such internal usage would not be subject to regulatory scrutiny.	criteria that could be included in the impact assessment, such as the differentiation between internal uses and consumer-facing applications, or the number of retail customers affected. EIOPA has also clarified that the supervisory expectations for low-risk AI systems will be very limited.
55	European Federation of Financial Advisers and Financial Intermediaries (FECIF)	We agree that a proportionate, risk-based approach should be applied to the use of AI systems. However, we believe that AI systems with a low impact on customers or business activities are in fact extremely limited and that due attention should therefore be paid to this proportionality mechanism if less stringent levels of governance and risk management are chosen.	Noted. EIOPA has also clarified that the supervisory expectations for low-risk AI systems will be very limited.
56	AMICE	The adoption of a risk-based approach is fundamental to ensure the effective governance of AI without stifling innovation. To better adhere to such approach, we suggest acknowledging that certain AI systems with no material impact for the clients or the insurance undertakings may be exempted from the application of certain governance measures, provided that the firms employing those AI systems retain full responsibility for their use. The suggested approach (empowering firms to determine which specific measures are necessary for each AI systems based on their own risk assessment) would also be more coherent with the exemptions of the AI Act (Article 6(3)).	Noted. See comment above.
57	Institute of International Finance	We welcome the recognition of the need to take into account risk-based and proportionality considerations as a guiding principle in this section of the Opinion. This differentiated approach is crucial for practical implementation. We support the consideration of 'Insurance-specific criteria' (para 3.4) including the extent to which an AI system impacts business continuity, financial position, legal obligations, and reputational risks. However, the statement that 'undertakings shall develop a combination of proportionate measures' (para 3.5) is inconsistent with the objective of the Opinion, and should be revised to use advisory rather than prescriptive language. The use of 'shall' is particularly problematic	Noted. The term "shall" has been removed from paragraph 3.5, but the term "should" has been kept since it is in line with similar guidance documents developed by EIOPA in the past. While not providing an exhaustive list, the Opinion

		as it creates mandatory obligations, but the word 'should' also creates quasi-requirements which are problematic. The Opinion should clearly distinguish between customer-facing use cases and internal use cases. The use of AI to support processes such as through employee-facing chatbots should normally be considered low-risk. The current approach is overly broad without this important distinction and could lead to significant wasted compliance expenditure. The Opinion should also consider the actual need to develop measures for all AI systems (given the broad definition of 'AI system' in the AI Act). Requiring extensive documentation for simple use cases (like using a large language model to summarise client service tickets, or voice recognition to transcribe live interactions) would be disproportionate. The Opinion fails to provide explicit exemptions for low-risk AI systems, implying that all applications must follow the same governance framework (with proportionality). It should clarify that companies (and the AMSB) can determine which risk management measures (if any) are necessary for each system. The Opinion should align with the AI Act's principle of exempting minimal-risk systems from certain requirements, particularly those performing narrow procedural tasks (Art. 6(3)). Furthermore, allow undertakings to leverage existing risk frameworks rather than creating parallel AI-specific structures, focusing on outcomes rather than process, is less prescriptive and more technology neutral. EIOPA should rigorously test whether any proposed granular guidance on AI Systems is firstly indeed sought by supervisors and secondly is going to be quickly outdated.	now includes further examples of the criteria that could be included in the impact assessment, such as the differentiation between internal uses and consumer-facing applications, or the number of retail customers affected. EIOPA has also clarified that the supervisory expectations for low-risk AI systems will be limited. Furthermore, it has also been clarified that the impact assessment should be limited in cases where AI systems are expected to have a limited impact. The Opinion has also clarified that when developing risk management systems in relation to AI systems, undertakings may leverage existing or updated frameworks, insofar as they reflect the key principles included in the Opinion. EIOPA will continue monitoring market developments via different tools, and it envisages to subsequently develop more detailed analysis on

			specific AI systems or issues arising from the use of AI systems in insurance and provide further guidance, as relevant.
58	Gesamtverband der Deutschen Versicherungswirtschaft	In general, we welcome the risk-based approach and the principle of proportionality. However, it would be helpful to clarify that compliance with existing legislation - particularly DORA, GDPR, IDD and Solvency II - fulfils the supervisory expectations for the responsible and risk-based use of AI systems. Additionally, it would be useful to clarify that this section is not intended to extend the requirements of the AI Act for high-risk AI to all AI applications. Furthermore, we consider EIOPA's approach of using examples to create clarity to be very challenging. It will be difficult to provide suitable examples for all sectors. To avoid confusion, it is best to avoid providing specific positive examples. On the other hand, a negative demarcation of clear cases that should not be included could be helpful and easier for companies to implement.	Noted. The Opinion has clarified that when developing risk management systems in relation to AI systems, undertakings may leverage existing or updated frameworks, insofar as they reflect the key principles included in the Opinion. The Opinion also clarifies that it does not set out new requirements and in particular it does not seek to alter the scope of the AI Act by extending the requirements of the AI Act for high-risk AI systems to all AI systems used in insurance. The examples have been retained to illustrate possible practical ways of implementing the principles outlined in the Opinion, but it is also highlight that undertakings need to develop governance and risks management

			measures that are adapted to the specific uses of AI systems.
59	CNP Assurances	CNP Assurances suggests providing more clarity on the concept of proportionality, whether it is related to the nature of the activity, the potential impact of the AI use case, or both. The extensive or limited use of AI systems will likely increase certain risks already identified in the risk mapping and create new risks. It is necessary to implement new risk management systems and adapt existing ones. Adapting risk management systems requires understanding levels of impact that are difficult to describe for AI systems, such as consumer vulnerability or reputational risk, which can affect the appropriate level of governance. An extension of the opinion on this issue would be beneficial. Regarding point 3.3, the potential negative impact of an AI system on non-discrimination should be described in broader terms, as discrimination is not the only possible consequence. "The potential negative impact of an AI system on the individuals involved" can stem from erroneous decisions or advice, discrimination, or lack of transparency, which may prevent effective challenges to the decision. It is suggested that personal data considerations be included in the impact assessment, along with a description of the legal and regulatory implications when such data is involved. Regarding point 3.6, the suggestion that a "reduction in the explainability of decisions and human oversight could be acceptable when the stakes are low" requires careful consideration. When personal data is involved, it is essential to explain the relevance of the processing and how it is conducted (both to the regulator and the individuals concerned). It is not relevant to suggest that an " alternative risk management measures such as data governance or human oversight may be developed to compensate their lack of explainability " ("black box" effect). Human surveillance can only be effective if the individual overseeing the AI system utput has sufficient information to critically assess the AI's work. Without an explanation of the reasoning or elements behind the AI's output, humans cannot perform quality control effectively (risk of "automation bias"), particularly when the AI results are generally perceived as accurate. The proportionality test needs clearer guidelines. It's essential to specify what elements it covers, such as documentation on bias absence, frameworks for unauthorized use cases, technical safeguards, and data sensitivity that can be processed with AI systems.	Noted. EIOPA has clarified that when developing the impact assessment undertakings should assess both the nature of the AI systems (e.g. complexity and autonomy) and its potential impact on customers and undertakings. The Opinion has also clarified that when developing risk management systems in relation to AI systems, undertakings may leverage existing or updated frameworks, insofar as they reflect the key principles included in the Opinion. The Opinion has also clarified the need to follow risk-based and proportionality measures in each of the principles outlined in the Opinion. The Opinion also acknowledges the importance of social dialogue and has explicitly mentioned this possibility in

		It is essential to evaluate the requirement to present specific AI system to employee representative bodies when the system is utilized by, or affects, employees. This assessment should ensure compliance with labour laws and mitigate potential criminal risks, such as charges of obstruction, in the event of non-compliance. Providing an explanation within the section of internal stakeholders during the implementation of a risk opinion on the measures could be helpful. Similarly, it may be relevant for AI systems suppliers to establish a quality label certifying the level of risk for certain pre-identified uses.	the text of the Human Oversight section.
60	IRSG	We appreciate EIOPA's endorsement of a risk-based approach and the emphasis on proportionality in AI governance and risk management. Indeed, these principles are fundamental to effective governance of AI systems, aligning with the existing framework. However, we would like to highlight two key considerations to further improve the practical application of these principles. First, while EIOPA's proposed impact assessment framework effectively identifies AI systems with limited impact on customers, the Opinion does not foresee any explicit exclusions from certain risk management and governance measures, as if their application would be required in all use cases, although with different degree of proportionality. We encourage EIOPA to acknowledge in its Opinion that insurance undertakings are responsible to decide which and how risk management measures need to be applied. Otherwise, the application of the full set of risk management and governance measures provided in the Opinion may be redundant and inappropriate for AI systems that, based on the impact assessment, demonstrate negligible or no risk for the company or its customers. In this respect, it's worth noting that the AI Act specifically provides exemptions for AI systems that do not pose "a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making" (Art. 6, par. 3). This consideration is particularly relevant with reference to data governance measures, whose application could be inappropriate for certain applications presenting no risks for the company or its customers. A more balanced approach would enhance proportionality and the risk that certain AI systems are not developed nor deployed due to overwhelming requirements. Second, while we agree that alternative risk management measures could be applied for AI systems lacking full explainability, such as those processing images, videos, or text, we recommend EIOPA to clarify that governance measures should vary significantly based on the actual risk of the specific application. In particular, adopting data governance and human oversight measures (either directly by the insurance company or indirectly by the insurance	Noted. A reference to the need to follow a risk-based and proportionate approach has now been clearly included at the beginning of each principle outlined in the Opinion. EIOPA has also clarified that the supervisory expectations for low-risk AI systems will be very limited. Furthermore, it has also been clarified that the impact assessment should be limited in cases where AI systems are expected to have a limited impact. The Opinion now explains that when conducting impact assessments, undertakings may differentiate between internal uses of AI systems that are not used for decision-making in processes that have a direct impact on consumers

		intermediary) may not be appropriate with reference to AI systems generating content strictly for internal purpose (e.g., images for internal presentations). The potential risks associated with these internal-use AI systems differ significantly from those of AI applications that impact directly the customers, such as AI systems providing core functions of pricing tools and claims management. Therefore, we recommend clearly distinguishing expectations between internal-use and low risks AI systems and other systems impacting customers, ensuring that governance and risk management measures remain proportionate to actual customer risks. This approach will allow the responsible development and management of AI systems without imposing extensive requirements and documentation based on theoretical or minimal risks. Having said that, this distinction between AI systems that impact the consumers and require greater control, versus those that do not, is not always easy to make. In any case, it should not lead to undervaluing the effect on consumers, nor the undertakings employees, even if indirect. Social dialogue at all levels represents an effective tool for addressing the impact of new technologies and digitalisation in the businesses. Finally, we would like to propose a change of pure detail in the wording of sect. 3.1: where it says ... 'In as similar line, Article 25 of the IDD...' it should refer not to undertakings in general, but to insurers and also to the intermediaries who manufacture products, as the article specifies.	and consumer-facing applications. Finally, the term "undertaking" used in the Opinion is generic, and covers both insurance undertakings and intermediaries.
61	CRO Forum	We support the emphasis placed on the need for a proportional and risk-based approach across the governance and risk management framework. Controls, oversight across the AI System lifecycle should be risk based and proportionate to the risk(s) presented by the AI system and take into account their adaptive and autonomous nature. EIOPA could explain the proportionality aspect even more clearly by recognising different requirements for (i) customer-facing versus internal use cases, and (ii) deployers versus providers. When considering risk factors for AI Use cases it is implied that processing large data sets can make an AI System riskier, but AI Systems' ability to process large data sets can also promote accuracy (as the AI Systems have larger data sets to learn and hone their accuracy on). (Paragraph 3.3) We support the assertion that insurance line of business has an impact on the level or proportionality of risk management required over an AI System. And a connection to Consumer Duty/Consumer Fair treatment could be emphasised here. We also support the consideration of an AI systems' impact on a firms' business continuity and prudential strength. EIOPA may want to make reference to the wider impact of AI System usage on the sector's sustainability as a whole, due to increased reliance on a relatively small number of AI System Infrastructure providers. (Paragraph 3.4 and Appendix 1).	Noted. The Opinion now explains that when conducting impact assessments, undertakings may differentiate between internal uses of AI systems that are not used for decision-making in processes that have a direct impact on consumers and consumer-facing applications. The trade-off between accuracy and explainability is also acknowledged in the Opinion.

		Given that AI Systems effectively learn and can improve accuracy or conversely drift over time, a sense of AI System maturity could also be considered when ensuring a risk-based approach and proportionality. Drift is the gradual decline in AI Model accuracy or reliability due to changes in the underlying data distribution. When the real-world data that a model encounters differs from the data it was trained on, the model output can become less accurate. In appendix 1/Point 1, the term 'human autonomy' could be replaced by 'human oversight'. 'Model transparency and explainability' could also be added as further means to assess impact. In appendix 1/Point 2, the table refers to 'high risk AI Use Cases' which have previously (in the scope section) been deemed out of scope for the Opinion paper. Inclusion in the appendix could therefore lead to confusion. In appendix 1 point 2, under the section on 'Reasons for using AI', as well as misuse of AI, we would suggest recognising that the benefits for an AI Systems use should not be outweighed by the cost of the AI Systems implementation and use. Ie. firms should be wary of solving low-cost business problems with expensive AI solutions. In appendix 1 point 2, under the section on 'staff involved in the design and implementation of the AI model', consider how staff running and oversighting an AI System will also need appropriate training, not just those who initially design and implement the AI System. In appendix 1 point 2, under the section on 'data collection', there could be greater recognition that documenting 'ground truth' is more challenging for the 'Off-the-shelf' AI models that are now available from suppliers. In appendix 1, section 3, under the section on 'demographic parity' the example might better suggest that interview candidate mix could also be judged fair if shortlisted candidates are proportional to the local population (as well as the number of applicants, as stated in the Opinion appendix).	A reference to the need to monitor model drift has also been included in the accuracy, robustness, and cybersecurity section of the Opinion. The reference in the Annex have not been amended given that they reflect the work of EIOPA's Consultative Expert Group on Digital Ethics in insurance. However, it has been clarified that they are included as illustrative examples and should not be considered as prescriptive guidance.
62	European Financial Congress	The opinion rightly emphasizes the need for risk assessment and proportionality of management measures depending on the scale and nature of AI use. However, the sheer necessity of conducting a risk assessment and documenting its results for each use case can be costly.	Noted. A reference to the need to follow a risk-based and proportionate approach has now been clearly included at the

		Worth considering: - Introducing simplified procedures for systems with minimal impact on customers and operations, - Reducing documentation requirements for simple use cases, - Clear guidance on minimum requirements for the lowest levels of risk, - Common risk assessment tools or templates available to the market, thereby reducing implementation costs.	beginning of each principle outlined in the Opinion. EIOPA has also clarified that the supervisory expectations for low-risk AI systems will be very limited. Furthermore, it has also been clarified that the impact assessment should be limited in cases where AI systems are expected to have a limited impact. EIOPA will provide high-level guidance, supplemented by illustrative examples in the Annex, and may develop more detailed guidance on specific AI systems or issues in the future, where relevant.
63	European Confederation of Institutes of Internal Auditing	There will likely be fewer single-use cases and more instances of autonomous systems, AI Agents, and orchestration layers. The impact on the risk assessment should be described, and guiding principles should be defined.	Noted. The principles-based nature of the Opinion and its emphasis on risk-based and proportionality considerations should allow the Opinion to be adaptable over time, but indeed EIOPA will continue monitoring market developments and provide further guidance, where relevant.
64	BETTER FINANCE	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	Noted. The Opinion acknowledges that there

		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".	are varying levels of risks among those AI systems that are not considered as high-risk or prohibited practices in the AI Act, and therefore undertakings should develop impact assessments to define risk-based and proportionate measures.
65	Actuarial Association of Europe	Key message: The AAE supports EIOPA's emphasis on a risk-based and proportionate approach. However, the Opinion could provide greater clarity on whether proportionality should relate to the nature of the business or to the potential impact of the AI use case. We also suggest acknowledging how AI may amplify certain risks and recommending additional contextual factors—such as consumer vulnerability or reputational risk—that may influence the appropriate level of governance. Detailed response: We welcome the Opinion's emphasis on a risk-based and proportionate approach, which is consistent with both the AI Act and existing supervisory frameworks like Solvency II. A flexible, principle-based application of proportionality is key to ensuring the framework can adapt to diverse business models and operational contexts across the insurance sector. However, the Opinion could provide clearer guidance on what the proportionality principle should be proportionate to. There appears to be an inconsistency between different regulatory perspectives: Solvency II focuses on the nature, scale, and complexity of operations, activities and the risks inherent in the business of (re)insurance undertakings, while other frameworks—including EIOPA's earlier work on digital ethics—suggest that proportionality should relate to the risk of harm to individuals. For example, a small insurer with limited operations might deploy an AI system in claims management that could materially affect policyholders' lives. Should proportionality in this case consider the insurer's size, or the impact of the AI application? Some of our members also believe that factors such as consumer vulnerability and financial literacy should inform proportionality assessments. These factors are relevant under the	Noted. EIOPA has clarified that when developing the impact assessment undertakings should assess both the nature of the AI systems (e.g. complexity and autonomy) and its potential impact on customers and undertakings. The Opinion follows a risk-based and proportionate approach, which should limit the impact on smaller undertakings and lower risk uses of AI systems. A reference to consumer vulnerability has been added to the text, in addition to the previous reference to the need to take into account the relevance of a line of business to the financial inclusion of customers. There are also references

		Insurance Distribution Directive and Product Oversight and Governance (POG) requirements and could be integrated here to support consistency. We also note that AI systems may amplify traditional risks, such as those related to fairness, explainability, and data quality. As such, proportionality should take into account not only the characteristics of the AI use case, but also the extent to which these risks may be intensified. Additional suggestions to improve the clarity and application of this section include: • Clarifying the meaning of proportionality in Paragraph 3.1 to distinguish whether it refers to business characteristics or AI-specific risks. • Incorporating a broader view of risk that includes not only solvency but also profitability and reputational impact. • Considering the evolving performance of AI systems and the need for forward-looking assessments, given the speed of technological change. • Ensuring that the discussion of image processing in Paragraph 3.6 reflects the potential for significant impacts, such as in claims handling. The current wording could be misinterpreted as suggesting such use cases are inherently low-risk. • Providing a clearer definition of terms such as "comprehensively explain", particularly where technical methods do exist to interpret outputs from image or text-based models. We also support the idea that insurers should regularly review and improve their AI risk management practices to avoid sudden or unexplained shifts in outcomes, thereby promoting operational stability and consumer trust.	to the potential reputational impact on undertakings, and in relation to the example of images, the Opinion acknowledges that there are trade-offs between accuracy and explainability, and therefore described in the example would be possible in certain AI systems, taking into account risk-based and proportionality considerations.
66	Insurance and Pensions - Denmark	See Q2 for proportionality and risk-based approach. Text specific comments: Point 3.4 (first part): “Insurance-specific criteria should also be tak-en into consideration, such as the extent to which an AI system is used in a line of business that is important for the financial inclusion of cus-tomers or if it is compulsory by law.” Comment: Financial inclusion is not mentioned on system level in Sol-vency II or IDD. We suggest that the wording on financial inclusion should be removed, or section marked as “additional consideration”. Point 3.4 (last sentence): “Reputational risks that could potentially arise from the use of AI	Noted. When analysing the potential impact on fair treatment of consumers, the financial inclusion of consumers can represent a valid factor to take into account, while at the same time it has been acknowledged that risk-based underwriting practices are allowed in insurance.

		systems in certain use cases should also be considered." Comment: It should be clear that reputational risk should not be an "automatic consideration" for all AI systems. It is only relevant in relation to the 'core insurance business' and, even then, only in scenarios of significant impact—for example, risk models or similar cases. It is less important for support activities and the auto-mation of tasks such as claims handling. Point 3.5: "As a second step, taking into account the nature, scale, and complexity of the AI use case at hand, undertakings shall develop a combination of proportionate measures that ensure the responsible use of the AI system. This implies that governance and risk management measures may be tailored to the specific AI use case […]" Comment: In the sentence "measures that ensure responsible use of AI systems", the word "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 [...]"	The criteria mentioned in the Opinion are not prescriptive, and should be considered where it is relevant taking into account risk-based and proportionality considerations. The term "responsible use" has been retained given that it is a widely recognized and established concept within the domain of AI governance, and it aligns with the principle-based approach of the Opinion.
67	Wind Tre S.p.A.	In addition to addressing governance and risk management measures for insurance companies, it is crucial to include insurance intermediaries in the regulatory framework. These intermediaries may integrate AI solutions during the product distribution phase, which could lead to overlapping governance frameworks. This overlap may arise from varying levels of risk between intermediaries and insurance undertakings, particularly concerning the proportionality principle and tailored governance measures highlighted earlier. To avoid fragmentation and ensure coherence, a harmonized approach should be pursued, or dedicated regulations developed. Such measures should recognize intermediaries as integral participants in the insurance value chain rather than treating them merely as third-party outsourcers, and they should reflect the specific nature, scale, and complexity of their AI use cases. Furthermore, the alignment of regulations across ICT governance and risk	Noted. The Opinion explains that its scope covers the activities of both insurance undertakings and intermediaries (jointly referred as 'undertakings'), insofar as they may use AI systems within their respective areas of competence in the insurance value chain.

		management frameworks, as seen in DORA, should be considered to prevent excessive burdens or misalignment. Taking into account the exclusion of prohibited and high-risk systems from the scope of the Opinion, the "levels of risk" mentioned in recital 3.2 will have to take into account and be consistent with the framework and requirements established by the AI Act in Chapters IV and V (which deal with Transparency obligations for providers and deployers of certain AI systems and general-purpose AI models).	The criteria mentioned in the Opinion is not prescriptive, and should be considered and complemented as relevant, taking into account risk-based and proportionality considerations
69	ANASF	We agree that a proportionate, risk-based approach should be applied to the use of AI systems. However, we believe that AI systems with a low impact on customers or business activities are in fact extremely limited and that due attention should therefore be paid to this proportionality mechanism if less stringent levels of governance and risk management are chosen.	Noted. EIOPA has clarified that the supervisory expectations for low-risk AI systems will be very limited. Furthermore, it has also been clarified that the impact assessment should be limited in cases where AI systems are expected to have a limited impact.
70	BEUC - The European Consumer Organisation	- Point 3.3. issues an open list of criteria to consider ("such as"), it would be preferable to have these criteria as minimum requirements ("including at least"). An open list gives too much leeway to the insurance company to decide which factors are taken into account. - Point 3.5: "The nature, scale and complexity of the AI use case" should be further defined to ensure that all potentially negative impacts for consumers are effectively mitigated. For example, the scale of the AI use case could be relatively small but still have a significant impact on consumers of a particular group, an AI system could be relatively simple but if the outcome of the AI decision-making is wrong (e.g. even a "simple" tool can establish wrong causalities), it comes with a strong negative impact for consumers. BEUC recommends categorising AI applications on the use of personal data (e.g. processes without use of personal data, processes with fully anonymised personal data, processes using personal data) and in addition to differentiate between processes which lead to a decision-making (e.g. on pricing, underwriting, claims handling, customer service) vs. back-end processes without involvement in the decision-making process. - Point 3.6: BEUC opposes to the sentence "More specifically, for certain AI use cases such as AI systems used to process images, videos, or text for which it is not possible to comprehensively explain how a certain output was obtained, alternative risk management	Noted. In line with the high-level and principle-based approach of the Opinion, the criteria are not meant to be prescriptive. EIOPA has aligned the terminology used across the Opinion and now refers to the need to take into account risk-based and proportionality considerations. Moreover, EIOPA has clarified that when developing the impact assessment undertakings should assess both the nature of the AI systems (e.g.

		measures such as data governance or human oversight may be developed to compensate their lack of explainability". It should be the responsibility of the insurance operator to ensure explainability (i.e. causality between the data input and the outcome in terms of decision made). Where such causality is non-existing or cannot be established, the risks of discrimination (e.g. for pricing/underwriting) are high. EIOPA opinion should not allow for such scenario. In addition, alternative risk management measures read currently as an option ("may") and are vaguely formulated which does not provide necessary safeguards for consumers.	complexity and autonomy) and its potential impact on customers and undertakings. Regarding the AI systems used to process images, videos, or text, the Opinion acknowledges that there are often trade-offs between accuracy and explainability, and therefore the proposed approach would be possible in certain AI systems, taking into account risk-based and proportionality considerations.
71	Spanish Association of Risk Management and Insurance, known as AGERS	Indicate risk profile and tolerance limits. List of processes and procedures. As part of the risk management system, identify more details of where, how, when and who uses AI in the company. Given its importance in the insurance sector, indicate the use made of the fundamental functions of Solvency II, in the Continuity Plan and in cases of outsourced activities. Together with risk identification, point out the benefits and advantages of using AI to balance potential harms and benefits. Pay special attention to the risk chain: supervision of subcontractors or third parties. Risk management frameworks should consider that the people involved in committees, forums, working groups, etc. have sufficient capacity to understand the models; It is important that there are no 'key man dependencies'; furthermore, AI-based models should be explicit about the hypotheses used; and, for example, justify in the appropriate forums that the pilots for the implementation of AI systems have been rigorous and deserve to move on to a second phase (which is not decided solely by the department of the AI user).	Noted. In line with the Opinion's Impact Assessment, EIOPA will focus on providing high-level guidance. This approach is complemented by specific examples included in the Annex. EIOPA will continue monitoring market developments and potentially develop further detailed guidance in the future, as relevant. The Opinion has also further explained that third-party service providers play a crucial role in AI

			governance, and highlighted the relevance of trainings for staff. The aspects mentioned about model training
72	AI & Partners	The risk-based approach is a practical framework for AI governance, ensuring that oversight measures are proportionate to the impact of AI use cases. However, insurers would benefit from clearer benchmarks or industry-wide standards for assessing AI risk. Encouraging collaboration with regulatory sandboxes could support proportional implementation while fostering innovation. Additionally, the Opinion could further emphasize the need for periodic reassessments, as AI systems evolve and potentially shift into higher-risk categories. More concrete examples of proportional risk management measures—such as tiered explainability requirements—would help insurers align their governance strategies with regulatory expectations.	Noted. In line with the Opinion's Impact Assessment, EIOPA will focus on providing high-level guidance. This approach is complemented by specific examples included in the Annex. EIOPA will continue monitoring market developments and potentially develop further detailed guidance in the future, as relevant. EIOPA will also continue to actively participate in the European Forum of Innovation Facilitators (EFIF), and monitor the implementation of the AI sandboxes foreseen in the AI Act.
		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?	
73	Mirko Kraft	Sustainability and environmental impact should be added to the list of areas (3.7): It should be taken into account that the use of an AI system may have a significant impact on the company's carbon emissions. This risk should always be assessed and, if found to be more than negligible in the medium to long term, the company should consider measures to mitigate the risk. A company that would report a doubling of energy consumption or massive layoffs due to the implementation of AI systems could face reputational damage that is not trivial. This is in line with Art. 46.2 of the Solvency II Directive.	Noted. At this stage, the environmental and social and employment impact of AI systems will not be considered as a separate criterion given that it is still an area of ongoing

		Social and employment impact should be also added to the list of areas (art. 3.7): the risk management framework should explicitly consider social and employment-related risks. It is recommended to incorporate factors such as job quality, psychosocial health, need of competence up-skilling and potential future changes in the business strategies. Technological change effecting privacy, working conditions, or data protection should include consultation with trade unions.	research and may be difficult to assess. However, the Opinion acknowledges the importance of social dialogue and has explicitly mentioned this possibility in the text of the Human Oversight section.
74	BIPAR	We do agree with the risk management section covering all aspects of data and tech management, especially on the point regarding staff of the undertaking having access to relevant training programs adequate to their respective roles and responsibilities. For IDD for example, the compulsory training should not add to the existing required of training in IDD. It would be useful to have some examples of when products have been adequately risk managed, especially in covering the ethical risk scenario. As done in other sections and for the sake of clarity, we believe that it would be necessary to refer in this section to the taking into account of risk-based and proportionality considerations. The draft Opinion does not distinguish between developers and deployers. This could result in distributors facing undue burdens, requiring them to extensively validate or duplicate controls already established by insurers or third-party developers. Intermediaries due to their size will mostly be deployers / users of systems which are developed by service providers. They must be able to rely upon the systems that are developed by service providers. Contractual requirements can cover this aspect. Intermediaries should be informed when insurers or product manufacturers use AI systems for the activities in scope. If there is no differentiation between developers and deployers, it would lead to double work in terms of controls already established by third-party developers. Lastly, regarding intermediaries, it should be reminded that art. 25.1 IDD states: “Insurance undertakings, as well as intermediaries which manufacture any insurance product for sale to customers, shall maintain, operate and review a process for the approval of each insurance product, or significant adaptations of an existing insurance product, before it is marketed or	Noted. The Opinion recognises that when developing risk management systems in relation to AI systems, undertakings may leverage on existing frameworks (including those related to staff trainings) insofar as they reflect the key principles included in the Opinion. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring.

		distributed to customers". Therefore, those who do not manufacture a product must receive all the information from those who do produce it	The Opinion also includes a reference of the need of insurance intermediaries to obtain sufficient information from insurance undertakings in order to meet their obligations towards customers.
75	Studio legale Floreani	The section on risk management may be enhanced by including specific guidance on the distribution segment, where multi-agency structures are prevalent. Risk governance requirements should be adaptable based on the intermediary's legal form, organisational structure, and risk profile, in line with the proportionality principle under both IDD and DORA. Moreover, the procurement and monitoring of third-party AI service providers should incorporate safeguards ensuring non-discriminatory practices, explainability, and compliance with relevant legal standards, including the GDPR, IDD, DORA, and AI Act. Recommended actions include: Incorporation of standardised contractual clauses for AI-related services. Deployment of structured due diligence checklists and ongoing monitoring tools., Definition of baseline risk management obligations for insurance distributors	Noted. The risk-based and proportionate approach of the Opinion allows for adopting the governance arrangements to different organisational structures, insofar as the key principles outlined in the Opinion are addressed. As previously explained, the Opinion is kept principle-based, with some specific and non-prescriptive examples in the Annex. More detailed guidance may be developed in the future where appropriate.
76	AFPA, Austrian Financial & Insurance Professionals Association	Bei der risikobasierten Unterteilung der KI-Systeme wird die Auslegung bei Grenzfällen immens wichtig sein. Aktuell spricht einiges dafür, dass sich bei der Aufbereitung der Informationen für das interne Risikomanagement unerwartete Fragestellungen ergeben werden und die unterschiedlichen Kategorisierungsansätze der verschiedenen Regelwerke zu widersprüchlichen Sichtweisen führen können bzw. werden. Daher werden hier noch erforderliche Anpassungen erwartet. Grundsätzlich muss KI ins bestehende Risikomanagement integriert werden. Wichtig sind praxisnahe, skalierbare Lösungen ohne übermäßige Bürokratie.	Noted. EIOPA has clarified that when developing risk management systems in relation to AI systems, undertakings may leverage existing or updated frameworks, insofar as they reflect the key principles included in the Opinion.

		In the risk-based classification of AI systems, the interpretation in borderline cases will be immensely important. Currently, there is much to suggest that unexpected questions will arise in the preparation of information for internal risk management, and the different categorization approaches of the various regulations can or will lead to conflicting viewpoints. Therefore, further adjustments are expected here. Fundamentally, AI must be integrated into existing risk management. Practical, scalable solutions without excessive bureaucracy are important.	As per the previous comment, further guidance may be provided in the future, where appropriate.
78	Insurance Europe	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.	Noted. The Opinion does not establish a supervisory checklist, but rather it follows a holistic approach to AI governance and risk management anchored in risk-based and proportionality considerations. The Opinion has clarified that the scope of the insurance sector legislation mentioned therein is not altered, and the principles outlined in the Opinion are applicable to the use of AI systems in insurance within the scope of the Opinion, based on requirements in sectoral legislation, and following a risk based and proportionate approach.
80	Lloyd's Market Association	We largely agree with the section on risk management systems, but would point out that not all of the areas which EIOPA state should be considered may be relevant for all AI use cases. We also believe that the Opinion should reinforce that AI risks may not require separate or siloed treatment, instead pointing out that AI risk management may be incorporated into	Noted. The Opinion recognises that when developing risk management systems in relation to AI systems, undertakings may leverage existing frameworks insofar as they reflect the key

		existing risk categories (e.g. model risk, conduct risk, outsourcing risk), with AI-specific nuances recognised through scenario analysis, impact assessments, and specialist controls.	principles included in the Opinion.
81	European Federation of Financial Advisers and Financial Intermediaries (FECIF)	We agree with the above statements, including those regarding the ongoing review process.	Noted.
82	AMICE	We believe that EIOPA's Opinion should incorporate the distinction between "deployer"" and "developer", as foreseen under the AI Act that does not contradict the ultimate responsibility of the outsourcing insurance undertakings set out under Solvency II. When insurers act as mere deployers, their main responsibility lies in ensuring proper implementation of the AI system in accordance with the instructions provided by the developer. Implying that an insurer must re-validate the underlying technology would be misaligned with the AI Act, duplicate efforts, and create unnecessary costs.	Noted. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring.
83	Institute of International Finance	The requirement that 'undertakings using AI systems within their organisation need to define and document in the relevant policy document … the approach to the use of AI within the organisation' creates new documentation requirements beyond existing frameworks. In our view, it is important to balance the ability to innovate with the evolution of safe and robust AI, considering the efforts and costs associated with providing the expected documentation. Streamlining this documentation is essential and would contribute to developing AI systems that are both robust and deliver economic benefits to consumers The language requiring 'accountability frameworks' and 'clearly defined' roles and responsibilities could be streamlined to leverage existing governance structures. Our members strongly believe that they don't need new mandatory risk management and governance frameworks for AI, although they are also keeping under review those frameworks in response to issues thrown up by new technologies. AI is one more tool that insurers are using and can be adapted into existing frameworks. They are of course ready to establish new mechanisms and controls as needed, and to keep existing frameworks flexible and adaptable. The Opinion should emphasize that proportionality applies not only to the areas of risk	Noted. The Opinion recognises that when developing risk management systems in relation to AI systems, undertakings may leverage existing frameworks insofar as they reflect the key principles included in the Opinion. The Opinion recognises that the principle of proportionality also applies to documentation and record keeping requirements.

		management and governance but also to the depth and formality of documentation required. A materiality threshold allowing simplified documentation for low-risk AI applications would support innovation while maintaining appropriate controls. The AI Act differentiates between developers, who must ensure compliance with technical and ethical standards, and deployers, who are responsible for appropriate implementation. Based on this distinction, EIOPA should explicitly recognize that insurers acquiring AI systems from third parties act as deployers, not developers. In such cases, while insurance undertakings retain the ultimate responsibility over the AI system employed, they should not be required to duplicate compliance assessments already conducted by AI developers. This means that when deploying a third-party AI system, insurance companies should be able to rely on the developer's assurances rather than independently verifying core functionalities, thereby avoiding disproportionate costs. Further, financial firms have reported difficulties in obtaining information from third parties about their AI technology—models, and training data in particular—which would be necessary for properly assessing and managing the associated risks. Indeed, some of our members report facing significant challenges with third-party AI vendors who may be hesitant to share critical information about their AI models, for commercial, litigation risk, or cybersecurity reasons, among others. This can create difficulties for FIs attempting to onboard and validate these systems. There may be scope for financial regulators to clarify regulatory expectations in such a way as to improve the position of FIs relative to model providers and support their ability to successfully leverage contractual frameworks to require third-party disclosure of vital information. It would be very helpful if the Opinion would also address this issue. The approach suggested in 2021 by EIOPA's Expert group report to classifying AI systems and their respective risk was reasonable. In our members' view this was truly guidance rather than being prescriptive in nature.	Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring.
84	Gesamtverband der Deutschen Versicherungswirtschaft	As we understand it, the section on the risk management system does not contain any new requirements and merely serves to clarify the existing regulatory framework. AI does not form a separate cluster, but as ICT it regularly falls within the scope of DORA. Risks for the company itself that may arise from the use of AI must be regularly included in the insurance company's risk management system. We also welcome that the section is kept generic, as there is no need for further specification	Noted. The reference to training has been maintained since this concept is commonly used in insurance legislation (e.g. IDD); the other statements mentioned in

		due to the existing comprehensive requirements for risk management of insurance companies (see, for example, Art. 44 SII Directive in conjunction with the downstream specifications for the design of the business organisation and risk management). In addition, however, a few points should be noted that (could) lead to misunderstandings: - The mention of 'trained programmes' in 3.10. is misleading, as an obligation already arises from Art. 4 of the AI Act. If this refers to AI literacy as defined in Art. 4 of the AI Act, the terminology must be adapted accordingly. - The term 'accountability framework' in 3.10. remains unclear, as it is neither found in DORA nor in the AI Act. In order to avoid misunderstandings, the opinion should not introduce any new terminology, but rather ensure standardised terminology (clear responsibilities, see Art. 5 para. 2 c DORA Regulation). - The term 'cross-references and dependencies' remains unclear. It should be clarified to which existing terminology is being referred. It should also be emphasised once again that no new requirements are intended. - The areas listed in 3.7. could be misinterpreted as going beyond the requirements of the AI Act for high-risk systems. It is necessary to clarify that this is not the case.	have been streamlined to clarify their meaning.
85	CNP Assurances	The approach here is also too general and generic. Regarding item 3.7, the list of areas where governance and risk management should be implemented should be accompanied by concrete examples of areas to be covered, mitigation measures and points of attention for each item. The formulation of more precise criteria for certain areas, and harmonised rules for their monitoring, can be useful for better risk management. The list of risk areas could be further expanded. In addition to technical and financial risks, insurers need to consider areas such as liability, sustainability performance and impact, as well as effective communication and internal collaboration, all of which are critical to embedding good AI governance. In the risk management system, general principles to be respected through controls must be clarified: 1. Alignment with the intended use;	Noted. The Opinion is kept principle-based, with some specific and non-prescriptive examples included in the Annex. More detailed guidance, such as the one included in the comment, may be developed in the future where appropriate. The controls described in the comment are generally in line with the documentation and record keeping example included in the Annex.

		2. The robustness and consistency of models and the settings made; 3. The implementation of appropriate performance metrics; 4. The implementation of tests on the different phases of the life cycle of models. Regarding point 3.9, the recommendation to frame the use of AI systems by policies and strategies seems quite relevant but too general. The document should illustrate the point with examples of points to be included in these policies and strategies (e.g. prohibited uses, need to systematically verify AI outputs, facilitate the reporting of difficulties encountered by AI systems users). The document should also emphasize that these policies and strategies need to be agreed at the highest level of organizations (to ensure their implementation) and reviewed regularly in view of the very rapidly evolving topics related to AIS. About point 3.10, CNP Assurances would like to stress that "the company's approach to AI systems" must be clearly defined and accompanied by clear usage policies for employees, regularly reviewed and monitored in their application. Further clarification on terminology, accountability and proportionality in communication and training would be useful. We suggest placing more emphasis on integrating AI into existing governance frameworks, rather than treating it as a separate topic, and aligning the AI Act benchmarks where appropriate. Finally, we suggest more clarity on the definition of roles and responsibilities in relation to this AI Act. Paragraph 3.10 refers to in-house and third-party models but does not reflect the distinctions of liability between AI system providers, deployers and other operators. Further alignment with the terminology and concepts outlined in the AI Act would provide greater clarity. CNP Assurances suggests a few measures concerning the risk management system for AI systems, such as: 1. Establish strict internal procedures (with a clear definition of the responsibility of the actors involved) to prevent AI systems from being designed and/or deployed without any prior analysis and so that an exhaustive mapping of these systems can be kept up to date. 2. Set up risk analysis grids to facilitate and standardise the carrying out of analyses, the solicitation of all the required expertise, carrying out regular reviews of analyses on this evolving subject.	The Opinion recognises that when developing risk management systems in relation to AI systems, undertakings may leverage existing frameworks insofar as they reflect the key principles included in the Opinion. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring.

		3. Risk monitoring is about the AIS actually deployed and is a key part of the "production" phase of the lifecycle. Controls at this stage should be recommended to ensure that AI systems are constantly under control in terms of, for example, quality and performance, data drift and bias, as well as data quality.	
86	IRSG	With reference to sect. 3.10, we note that EIOPA does not appear to consider cases where an insurance company acquires an AI system from a third party, thereby acting solely as a deployer rather than a developer. While the Solvency II framework assigns overarching responsibility to the insurance undertakings, even when outsourcing core functions, the AI Act introduces a clear distinction between the responsibilities of developers and deployers. Specifically, the AI Act establishes that primary accountability for ensuring compliance with core technical, safety and ethical standards resides with the AI developer, while deployers are responsible primarily for the appropriate implementation and usage context. This distinction is crucial and should be explicitly acknowledged in the Opinion, as the responsibilities and risk management obligations of a company deploying a third-party AI system differ significantly from those of a company that develops such a system in-house. Failure to differentiate between developers and deployers could result in undertakings facing undue burdens, requiring them to extensively validate or duplicate controls already established by third-party developers. I. e., if an undertaking deploys a third-party AI tool for fraud detection, it should reasonably rely on the developer's assurance regarding the core functionalities and compliance of the system. Requiring insurers to independently verify and document the detailed internal workings or training methodologies of third-party systems would create impractical and redundant obligations, without corresponding consumer benefits. Regarding the intermediaries, it should be borne in mind that art. 25.1 IDD states: "Insurance undertakings, as well as intermediaries which manufacture any insurance product for sale to customers, shall maintain, operate and review a process for the approval of each insurance product, or significant adaptations of an existing insurance product, before it is marketed or distributed to customers". Therefore, those who do not manufacture a product must receive all the information from those who do produce it. The omission to differentiate between developers and deployers is a recurring issue throughout the Opinion, and we suggest EIOPA to provide a clearer distinction between the two roles. To this end, we suggest rewording sect. 3.10 as follows: "The approach to AI systems should also include accountability frameworks, regardless of whether the AI system	Noted. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring. The Opinion also includes a reference to the need of insurance intermediaries to obtain sufficient information from insurance undertakings in order to meet their obligations towards customers. The Opinion also includes a reference to social dialogue and recognises the importance of providing relevant training to staff.

		is developed in-house or in collaboration with third parties, where the roles and responsibilities of different staff are clearly defined (see also…). However, where an AI system is acquired from a third party, undertakings' oversight responsibilities should focus on its appropriate deployment and integration, rather than duplicating technical validation obligations that remain with the developer under the AI Act […]". Establishing this distinction would help ensure that risk management requirements are appropriately allocated, preventing undue burdens on deployers while maintaining accountability for AI system performance and compliance. It should be made clear that the distinction between deployers and developers is made for regulatory and operational purposes, not in relation to (potential) customers, who are a third-party, alien to the relationship between the insurer and its provider, if the former is merely a deployer. This means that the company's liability towards the customer does not change, nor can it argue to the customer that it did not develop the AI system from which damage may have arisen. Otherwise, it would be sufficient to outsource this service to free itself from any liability, which is obviously unacceptable. On the contrary, the insurer is liable when it outsources this activity in the same way as any other, within the framework of art. 49 Solvency II. The sect. 3.10 also refers to the relationship between companies and staff in the use of AI, to conclude that they must be adequately trained, specifically in relation to fairness and ethical considerations. But in practice, employees are faced with training needs on everything from the use of digital tools to the need to know their company's policy on the use of AI, as well as regulatory knowledge. Having employees capable of identifying and mitigating risks of misuse, unethical outcomes, potential biases, inaccuracies, and data and security breaches is essential to strengthen AI-related 'first line' risk management. Social and employment impact should be added to the list of art. 3.7: the risk management framework should explicitly consider social and employment-related risks. We recommend incorporating factors such as job quality, psychosocial health, need of competence up-skilling and potential future changes in the business strategies. Technological change effecting privacy, working conditions, or data protection should include consultation with trade unions.	
87	CRO Forum	In paragraph 3.8 the Opinion recommends the use of the web of elements from a firm's existing risk management approach (e.g. fairness, ethics and data governance) but paragraph 3.9 seems to require a discrete policy document covering AI use. Firms can apply their existing framework of governance and risk management requirements and therefore may not need a discrete reference to AI management in policy documents, particularly in	Noted. The Opinion recognises that when developing risk management systems in relation to AI systems,

		smaller firms or firms where the introduction of AI is limited or low key. The Opinion should emphasise that proportionality should also apply to the depth of documentation required.	undertakings may leverage existing frameworks insofar as they reflect the key principles included in the Opinion.
88	European Financial Congress	The opinion mandates that AI be incorporated into existing risk management systems and that policies and procedures be regularly updated. Companies are also expected to document their approach to AI and assign responsibilities. From the industry perspective, it is worth considering: - possibility to use existing procedures (e.g., IT, data) without creating new ones dedicated solely to AI, - limiting the frequency of reviews to situations where the scale or nature of AI use actually changes.	Noted. The Opinion recognises that when developing risk management systems in relation to AI systems, undertakings may leverage existing frameworks insofar as they reflect the key principles included in the Opinion. The Opinion also clarifies that undertaking's approach to AI systems should be regularly reviewed, in particular if the number, type and materiality of AI systems used within the organisation changes.
89	European Confederation of Institutes of Internal Auditing	The IIA is promoting the 3 lines model as a key tool to strong corporate governance articulating the core components of effective governance: *Accountability by a governing body to stakeholders for organisational oversight; *Actions, including risk management, by management to achieve the objectives of the organisation through risk based approach; *Assurance, insight and advice by an independent internal audit function to provide clarity and confidence, and to promote and facilitate continuous improvement.The model is available on www.theiia.org /glob-three-lines-model-paper_layout-rebuild. It is important to define the way to evaluate the systems and the role of the different actors to support the strategy and reduce risks.	Noted. The Opinion acknowledges the importance of the audit function and includes a explicit reference to them in the Human Oversight section. The Opinion has also clarified that when developing risk management systems for AI systems, undertakings

		In this context, the Internal audit department plays an important role in assisting the audit committee in this duty. As we provide independent and objective assurance and insight on the internal control systems, the governance and risk management. We also assess the other Lines and give an integrated opinion. Finally, we make recommendations, after discussion with Management, and follow up on the implementation of these actions. The policy document should not be limited to strategy documents. It should also describe the approach, governance, and controls for the first, second, and third lines.	may leverage on existing frameworks (not only strategy documents) insofar as they reflect the key principles outlined in the Opinion.
90	Federation of European Risk Management Associations (FERMA)	FERMA agrees with EIOPA's opinion on this issue. We would also recommend that risk profiles and risk appetite for AI systems are clearly defined in the relevant policy document. Moreover, an AI risk management system needs to follow an enterprise-wide risk management (ERM) approach, taking into account the different AI system deployed in the undertaking both separately and as a whole. This is necessary in order to assess the overall AI-risk exposure of the undertaking and ensure that appropriate prevention and mitigation measures are implemented at the enterprise level. Third-party AI-related risks should also be carefully monitored. Additionally, undertakings should also ensure that users are trained to mitigate the risks of misuse, unethical outcomes, potential biases, inaccuracy and data and security breaches. Committee members tasked with AI oversight should understand AI models and avoid single-person dependencies. Approval for the deployment of AI models should follow rigorous processes that go beyond the department in which the system is deployed.	Noted. The Opinion has clarified that when developing risk management systems for AI systems, undertakings may leverage on existing frameworks insofar as they reflect the key principles outlined in the Opinion. The Opinion also recognises the importance of adequate training for the relevant staff.
91	BETTER FINANCE	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.	Noted. The environmental impact of AI systems has not been considered as a separate criterion at this stage, due to ongoing research and potential assessment difficulties. Further input is being collected on this topic through an on-going Generative AI market survey.

		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.	Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring.
92	Actuarial Association of Europe	Key message: The AAE supports EIOPA's approach to integrating AI-related risks within the existing risk management system. However, it would be helpful to provide additional clarification on terminology, accountability, and proportionality in communication and training. We suggest placing greater emphasis on embedding AI within existing governance frameworks, rather than treating it as a separate topic, and aligning references with the AI Act where appropriate. Detailed response: Many of our members stressed that AI risks should not be treated in isolation but rather incorporated into the broader enterprise risk management framework. This reflects the reality that AI is a tool—albeit a powerful one—and not a standalone category of risk. A more integrated approach would also support proportionality in practice. We support the integration of AI-related risks into insurers' overall risk management systems, consistent with the principle of proportionality and alignment with Solvency II. In some jurisdictions, such as Germany, similar expectations already exist under national supervisory	Noted. The Opinion has clarified that when developing risk management systems for AI systems, undertakings may leverage on existing frameworks insofar as they reflect the key principles outlined in the Opinion. Furthermore, in accordance with its principle-based approach, no preference is given as to which policy document should be developed. Concerning third parties, the Opinion clarifies that undertakings are

		guidance (c.f., BaFin paper of June 2021 titled “Big Data and Artificial Intelligence: Principles for the Use of Algorithms in Decision-Making-Processes”). In that context, the Opinion could be clearer in distinguishing between when new policies or frameworks are needed versus when existing ones can be extended. For example, Paragraph 3.9 mentions “a specific AI strategy” as an illustrative policy. It may be more helpful to refer to “an AI strategy or an integrated model governance policy” to reflect the option of embedding AI governance within existing structures. We also believe that accountability should be clearly defined and tied to the roles articulated in the AI Act. Paragraph 3.10 refers to in-house and third-party models but does not reflect the accountability distinctions between AI system providers, deployers, and other operators. Further alignment with the terminology and concepts of the AI Act would improve clarity. On the topic of organisational responsibilities, we propose that undertakings should establish clear accountability at senior management level. One option might be to designate a Chief AI Officer (CAIO), potentially combining this role with another executive position provided the necessary expertise is present. Actuaries may be well-suited to support or contribute to this function given their skills in data analysis and risk governance. Training and communication are also key elements. We suggest that requirements to communicate AI governance policies to “all staff” (as stated in Paragraph 3.10) may be disproportionate. Instead, policies should be communicated to all relevant staff who are reasonably expected to engage with or be affected by the AI systems. Relatedly, clarification is needed around who should receive training, and when. For example, staff implications will differ depending on whether an AI system is integrated into an existing pricing model, or whether a generative AI tool is rolled out company-wide. We also propose expanding the list of risk areas in Paragraph 3.7. In addition to technical and financial risks, insurers should consider areas such as accountability, effective communication, and internal collaboration, all of which are essential to embedding sound AI governance. To support risk management practice, clearer definitions of “accuracy” and “robustness” would be welcome. Moreover, the scope of material risks should extend beyond solvency to include profitability, reputational impacts, and effects on core processes such as underwriting and claims.	responsible for the AI systems they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring. The Opinion recognises in the Human Oversight section the important role played by the Administrative, management or supervisory body (AMSB) members. The Opinion has clarified that trainings should be provided to “relevant” staff. The Opinion has also been streamlined in the relevant parts to clarify the text, including with examples of accuracy metrics and including explicit references to model drift.

		Finally, we agree that risk management practices should be dynamic. Paragraph 3.9 could highlight the need to review AI approaches when systems already in use begin to exhibit unforeseen behaviour, as may happen with automated learning models. This would encourage ongoing vigilance and responsiveness.	
93	Insurance and Pensions - Denmark	The section refers both to Solvency II, IDD and DORA as legal basis. To avoid unnecessary burdens by extending the scope of the three regula-tions to use cases, that are out of scope, the specific ele-ments/considerations in the section should be clearly marked as to whether they apply in light of IDD or Solvency II. It should also be made clear that use cases that are out of scope of the regulations are not included in the supervisory expectations, and that any recommendations here are purely inspirational. Text specific comments: Point 3.7: It could be considered to mark the bullets “Fairness and ethics” with a “where relevant” or “additional considerations”, as fairness and ethics are not covered by Solvency II or IDD at system level. IDD covers fair-ness (not ethics) only in scope of insurance distribution. For clarity the limited extend of scope – especially in relation to IDD - should be made clear. Point 3.9: “Undertakings using AI systems within their organisation need to define and document in the relevant policy document (e.g. IT strategy, data strategy or a specific AI strategy) the approach to the use of AI within the organisation, including the governance and risk man-agement measures that should be developed throughout the lifecycle of an AI system. This approach should be regularly reviewed, in particular if the number, type and materiality of AI systems used within the organ-isation changes.” Comment: It should be emphasized that this only applies to the insur-ance business in scope of Solvency II (not IDD). Non-related / supplementing operations would not be covered. I.e. sim-ple grammar and spellchecks of texts where context is not changed or use of AI pictures for a presentation.	Noted. The Opinion has clarified that the scope of the insurance sector legislation mentioned therein is not altered, and the principles outlined in the Opinion are applicable to the use of AI systems in insurance within the scope of the Opinion, based on requirements in sectoral legislation, and following a risk based and proportionate approach. Furthermore, as highlighted in the Opinion, governance and risk management measures need to be adapted to specific uses of AI systems, which, for instance, would enable avoiding placing excessive emphasis on fairness and ethical considerations on purely prudential AI systems with no direct impact on customers. The Opinion has also clarified that when developing risk

		Point 3.10: “The undertaking’s approach to AI systems, which should include fairness and ethical considerations, should be communicated to the staff of the undertaking, who should have access to relevant training programs adequate to their respective roles and responsibilities.” Comment: The sentence above is not covered by Solvency II, IDD or DORA at system level. It should be removed or clearly marked as "additional considerations."	management systems for AI systems, undertakings may leverage on existing frameworks insofar as they reflect the key principles outlined in the Opinion.
94	Wind Tre S.p.A.	In the wording of this paragraph, in accordance with the provisions of the AI Act, undertakings should be distinguished in more detail, taking into account the different roles between providers and deployers of AI systems. In fact, risk management also depends on these roles. The risk management measures must be consistent and proportionate (taking into account the actual risk) with the measures provided for in art. 9 of the AI Act for high-risk systems.	Noted. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring. The risk management measures outlined in the Opinion are indeed expected to be implemented following a risk-based and proportionate approach.
96	ANASF	We agree with the above statements, including those regarding the ongoing review process.	Noted.
97	BEUC - The European Consumer Organisation	-Point 3.10: Risk management systems need clearly define who is accountable and liable in case of mistakes made by the AI system. Accountability and liability for certain staff categories should not discourage or disincentivise human intervention in the decision-making of the AI system.	Noted. The Opinion specifies that roles and responsibilities of different staff and the interplay between them should be clearly defined.

98	Spanish Association of Risk Management and Insurance, known as AGERS	Indicate risk profile and tolerance limits. List of processes and procedures. As part of the risk management system, identify more details of where, how, when and who uses AI in the company. Given its importance in the insurance sector, indicate the use made of the fundamental functions of Solvency II, in the Continuity Plan and in cases of outsourced activities. Together with risk identification, point out the benefits and advantages of using AI to balance potential harms and benefits. Pay special attention to the risk chain: supervision of subcontractors or third parties. Risk management frameworks should consider that the people involved in committees, forums, working groups, etc. have sufficient capacity to understand the models; It is important that there are no 'key man dependencies'; furthermore, AI-based models should be explicit about the hypotheses used; and, for example, justify in the appropriate forums that the pilots for the implementation of AI systems have been rigorous and deserve to move on to a second phase (which is not decided solely by the department of the AI user).	Noted. The Opinion is kept principle-based, with some specific and non-prescriptive examples included in the Annex. More detailed guidance could be developed in the future, where appropriate. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring.
99	Chika Okoli	Observation: Similar to the EU DORA compliance requirements, I think that Critical Third Party (CTP) risk management ought to be addressed a bit more directly to account for AI risk among CTPs to ward off systemic contagion. Suggestion: An approach could be to ask firms to map and identify AI deployment among CTPs i.e. the existing CTP register for EU DORA could have a column for material AI use by CTPs to avoid creating duplicate registers. Benefit:	Noted. In line with its principle-based approach and taking into account the on-going work in DORA concerning critical third parties, the Opinion does explicitly mention the latter, but undertakings are asked to have adequate and up-to-date IT infrastructure as well as fall-back plans to ensure ICT business continuity.

		This would provide authorities with visibility of the AI risk exposure among CTPs to anticipate the impact of AI risks and the resultant continuity issues.	
100	AI & Partners	The Opinion provides a solid foundation for AI risk management, emphasizing fairness, transparency, and cybersecurity. However, it could further address the challenges of integrating AI governance into existing enterprise risk management (ERM) frameworks. Clearer guidance on balancing explainability with model complexity—particularly for deep learning applications—would support practical implementation. Additionally, the introduction of standardized industry frameworks for AI risk assessment, similar to those in financial stress testing, could enhance consistency across insurers. Encouraging cross-sector collaboration between insurers, regulators, and AI ethics boards could also foster best practices in AI risk governance.	Noted. The Opinion explains that when developing risk management systems for AI systems, undertakings may leverage on existing frameworks insofar as they reflect the key principles outlined in the Opinion. The Opinion also acknowledges the trade-off between accuracy and explainability and emphasises the need to follow a risk-based and proportionate approach. The Opinion is kept principle-based, but EIOPA will conduct further assessments in the future in close collaboration with stakeholders and provide more detailed guidance, where relevant.
		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?	
101	Mirko Kraft	It is important to distinguish between discrimination and differentiation, a core principle of the insurance industry. Differentiation is the practice of setting premiums based on the level of risk posed by each policyholder. A crucial aspect of this practice is actuarial fairness, which ensures that individuals with the same risk profile pay the same amount. It is well known that the use of AI has facilitated a better determination of the risk posed by each individual seeking insurance. As long as this happens, it is legitimate, even if it means that more people	Noted. The Opinion now includes an explicit reference to risk-based underwriting practices in insurance. A reference to

		are left uninsured or have to pay a higher premium than before this level of precision was achieved.	actuarial fairness has also been added in the Annex.
102	BIPAR	We understand that EIOPA is ensuring that undertakings focus on the customer, but for some intermediaries, customer also mean for example corporates or insurers. It might be useful to define what “customer-centricity” (see point 3.12) means for B2B players in this industry. The phrase ‘Free of bias’ (see point 3.13) could be controversial, especially when most companies in the sector are not developing their Generative AI models. Perhaps EIOPA could provide some clarity on bias-reduction instead? We believe addressing the prohibited and also high risk AI systems could bring up important findings regarding the fairness and ethic aspects of AI usage. This will create an opportunity to set some acceptability limits for certain models or use cases which may fall in the grey area. For example, behavioural based insurance products were seen as a potential opportunity for the development of new products and solutions for the clients. To what extent a telematic insurance product, using AI processed data on the driving style of a person, can be considered as generating a social score effect (as described in the AI Act section for prohibited AI systems) for clients who have a driving style which is different from what the algorithm sees as acceptable ? Such a client could end up no longer receiving an offer from that carrier. Moreover, in case he/she has agreed in the terms and conditions that his/her history of driving score can be shared with other players (without being really aware of such an agreement), the client could end up excluded by several carriers. Lastly, it must be noted that the principle of pursuing the best interest of the customer, as referenced by EIOPA in section 3.12 and derived from the IDD framework, is not relevant in cases where AI systems are used exclusively for internal purposes, with no direct or indirect effect on end customers. This should be clarified in EIOPA Opinion.	Noted. The Opinion highlight that governance and risk management measures need to be adapted to specific uses of AI systems, which, for instance, would enable avoiding placing excessive emphasis non-discrimination issues in the case of B2B customers or for purely internal purposes that do not involve decision-making with a direct customer impact. In addition, while noting that certain variables need to be used to underwrite risks in insurance, the Opinion clarifies that undertakings should make reasonable efforts to remove biases in the data, including potential unlawful proxy discriminatory variables. The objective of EIOPA’s Opinion is to provide further clarity on the main principles and requirements foreseen in the insurance sectoral legislation and not on the AI Act. The European

			Commission has recently published Guidelines on prohibited AI practices under the AI Act.
103	Studio legale Floreani	Further clarification is needed on obligations regarding fairness and ethical use of AI in insurance distribution, particularly in ensuring transparency for clients. AI-based outputs should be clearly explainable using appropriate methodologies (e.g. LIME, SHAP), and clients should be empowered to contest automated decisions where applicable. To this end, it is recommended to: Adopt standardised models for algorithmic transparency. Introduce mechanisms for regular bias testing and independent audit. Ensure reporting obligations are proportionate to the distributor's size and complexity.	Noted. The Transparency and explainability section of the Opinion already includes references to the methodologies mentioned in the comment and to redress mechanisms. As previously explained, the Opinion is kept principle-based, with some specific and non-prescriptive examples included in the Annex. More detailed guidance may be developed in the future, where appropriate.
104	AFPA, Austrian Financial & Insurance Professionals Association	Fairness und Ethik beim Einsatz von KI-Systemen sind essenziell – nicht nur im technischen Sinne, sondern als gesamtgesellschaftliche Aufgabe. Es reicht nicht, die Verantwortung allein auf die Systeme oder ihre Entwickler abzuwälzen. Die Frage, was „fair“ ist, kann nicht von Algorithmen beantwortet werden, sondern muss durch gesellschaftlichen Konsens, politische Leitplanken und die Wertehaltung der Unternehmen getragen werden. Eine Schaffung von Awareness in der Bevölkerung ist zwingend notwendig. KI-Systeme sind als größte technische Revolution in der Geschichte der Menschheit anzusehen. Jeder Bereich des menschlichen Zusammenlebens wird davon betroffen sein und somit muss auch jeder Bereich neu bewertet werden. Wie oben bereits angerissen, wird hier entscheidend sein, inwieweit die KI-System-Anbieter an einer umfangreichen Aufbereitung der Informationen mitwirken. Entscheidend wird sein, wie die Aufsicht reagiert, wenn der Anbieter schleppend bzw. unzureichend mitwirkt, es sich aber um marktbeherrschende Tools bzw. Systeme handelt.	Noted. The Annex of the Opinion acknowledges that there are different types of fairness metrics, which might be different from one use case to another. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for

		Hier kann es bei einer restriktiven Vorgehensweise der Behörde durchaus zu Nachteilen für den europäischen Markt kommen. Das Betreten des Marktes durch außereuropäische Anbieter wäre eine mögliche Konsequenz. Grundsätzlich stellt sich aber die Frage, ob nicht ein „Recht auf menschliche Beratung“ Einzug halten sollte, und somit den Kunden eine Chance auf eine persönliche Beratung einräumt. Das würde ebenfalls den europäischen Markt stärken. Fairness and ethics in the use of AI systems are essential—not only in a technical sense but as a societal task. It is not enough to shift the responsibility solely onto the systems or their developers. The question of what is "fair" cannot be answered by algorithms but must be supported by societal consensus, political guidelines, and the values of companies. Raising awareness among the population is imperative. AI systems are to be regarded as the greatest technical revolution in human history. Every area of human coexistence will be affected, and thus every area must be re-evaluated. As mentioned above, it will be crucial to what extent AI system providers participate in the comprehensive preparation of information. It will be decisive how the supervisory authority reacts if the provider participates hesitantly or inadequately, but the tools or systems are market-dominant. Here, a restrictive approach by the authority could indeed lead to disadvantages for the European market. The entry of non-European providers into the market would be a possible consequence. Fundamentally, the question arises whether a "right to human consultation" should be established, thus granting customers the opportunity for personal advice. This would also strengthen the European market.	instance through contract clauses, audits, and monitoring. Concerning the right to Human intervention, while not covered by the present Opinion, the General Data Protection Regulation recognises individuals the right to not be subject to decisions based solely on automated processing.
106	Insurance Europe	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”.	Noted. The Opinion has clarified that the principles outlined in the Opinion remain applicable to the use of AI systems in insurance, since similar principles underline sectoral legislation. It also recognises that risk management measures for AI systems should be proportionate to their use, which implies placing less emphasis on fairness and ethics for systems that

		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.	don't affect customers directly. In addition, while noting that certain variables need to be used to underwrite risks in insurance, the Opinion clarifies that undertakings should make reasonable efforts to remove biases in the data, including potential unlawful proxy discriminatory variables. The Opinion acknowledges that different uses of AI systems may require different fairness metrics and has clarified that the examples included in Annex I are not meant to be prescriptive guidance. The Opinion also now includes references to risk-based underwriting practices.
108	Lloyd's Market Association	We believe that paragraph 3.12 does not change the current position – undertakings should already be ensuring that customers are treated fairly. We would therefore welcome explicit recognition that, where undertakings already comply with established obligations, only targeted adjustments, rather than wholesale changes, may be required. We generally agree that AI outcomes which impact customers directly should be regularly monitored and audited where possible, always in line with proportionality principles. It is important that the rules around conduct and customer interactions are outcomes based.	Noted. The Opinion explains that when developing risk management systems for AI systems, undertakings may leverage on existing frameworks insofar as they reflect the key principles outlined in the Opinion.

		Paragraph 3.15 addresses redress systems. However, we do not think that a specific redress mechanism needs to be implemented in relation to AI usage, as insurers will already have avenues through which customers can complain. We also think the reference to customers being “negatively affected” by an AI system is unhelpful. “Negatively affected” can have a variety of meanings. There will be instances, for example, where a customer may be negatively affected by an AI system, but should not have access to any redress mechanism such as where AI engaged in insurance pricing and risk selection has generated increased premiums based on non biased, non discriminatory data. A customer may perceive themselves as having been “negatively affected” because of the increased premium but that would, in that instance, have been produced by entirely ethical means. We would therefore recommend that paragraph 3.15 be amended to recognise existing redress mechanisms and to remove the reference to when customers can use them i.e. remove the reference to “negatively affected”.	The Opinion has clarified that redress mechanisms do not need to be specific to AI systems; complaints mechanisms that undertakings already have in place would normally suffice to enable customers to seek redress when they have been harmed by the use of an AI system in insurance
109	European Federation of Financial Advisers and Financial Intermediaries (FECIF)	FECIF agrees with EIOPA's comments regarding the fairness of AI systems and ethics, and the provision of adequate redress mechanisms to enable customers to seek compensation if they have been harmed. It is important that firms are aware that they will be responsible for the AI systems they implement.	Noted.
110	AMICE	The IDD’s principle of acting in the best interest of the customer may not be relevant for AI systems that are used exclusively for internal and non-insurance processes. Therefore, we suggest acknowledging that governance requirements should be scaled proportionally based on the actual impact of the AI system. On discrimination, we agree with EIOPA’s stance but emphasize the need to differentiate between "discrimination" and "differentiation": whereas differentiation is used to set premiums based on risk, discrimination involves illegal factors like race or gender. In this perspective, differentiation may be considered as “biased” only when it turns into discrimination.	Noted. The Opinion explains that the proportionality principle is applicable to all the governance and risk management measures described in the Opinion. The Opinion now includes an explicit reference to risk-based underwriting practices in insurance and highlights the need to prevent the use of unlawful proxy discriminatory variables.
111	Institute of International Finance	In para 3.11 EIOPA cites the IDD principle requiring insurance distributors to act in the customer’s best interest. The application of this principle is relevant for AI systems that impact the customer, directly or indirectly. However, the application of the same approach	Noted. The Opinion recognises that governance and risk

		does not seem appropriate for AI systems used only for internal purposes. EIOPA should take into account this difference and better specify the scope of application of the abovementioned principle. The requirement to develop 'a corporate culture that includes ethics and fairness guidance and relevant trainings' (para 3.12) extends beyond the proper scope of an Opinion on AI. This is adequately covered by other EIOPA or competent authority material. To the extent it is not already so covered, we would not support its inclusion in this paper. The Opinion's statement that training data 'is accurate, complete, representative and free of bias' (para 3.13) presumably means 'should be' and as such creates a new standard rather than merely guidance. Furthermore, it should be pointed out that the guidance on data quality and monitoring for fairness and non-discrimination (paras 3.13 and 3.14) should be scaled based on the AI system's actual impact on insurers and customers. Imposing uniform expectations on all AI applications could unnecessarily constrain low-risk systems, potentially hindering innovation without tangible ethical or fairness benefits. EIOPA should restate in this section the application of the proportionality principle, by introducing a more tailored approach. The expression 'negatively affected by an AI system' (para 3.15) is very broad and open to a wide range of interpretations. This language should be reconsidered or clarified.	management of AI systems should be proportionate to their use, which for instance would enable placing less emphasis on fairness and ethics for systems that don't affect customers directly. The Opinion is consistent with the underlying principles of sectoral legislation and no regulatory gaps have been identified. Indeed the Opinion now clarifies that training and testing data should be accurate, complete, and appropriate. The Opinion now refers to redress mechanisms which can be used by customers when they have been harmed by the use of an AI system in insurance.
112	Mathias Lindholm, Associate Professor of Mathematical Statistics, Stockholm University, Sweden. Ronald Richman, CEO, insureAI, and Chair, ASTIN Board, South	We recommend adding explicit supervisory expectations on the detection and mitigation of proxy discrimination, which is currently not referred to in Annex I. Proxy discrimination arises when sensitive policyholder characteristics (e.g. ethnicity), whose use is not permitted in insurance pricing, are indirectly inferred from other characteristics (e.g. postal code) that are considered legitimate. Proxy discrimination can take place implicitly and unintentionally by the prediction algorithms used, encompassing AI models but also more traditional statistical techniques. While this is not specific to AI, AI allows the extensive use of individualised policyholder data, which can lead to more intense proxying effects.	Noted. The Opinion now clarifies that undertakings should make reasonable efforts to remove potential unlawful proxy discriminatory variables. Concerning the fairness metrics included in the

	Africa. Andreas Tsanakas, Professor of Risk Management, City St George's, University of London, United Kingdom. Mario V. Wüthrich, Professor of Mathematics, ETH Zurich, Switzerland.	As such indirect use of protected characteristics defeats the point of banning their direct use, the detection and mitigation of proxy discrimination should be the baseline fairness safeguard for insurance pricing, before considering group fairness. As datasets grow richer, models can increasingly reconstruct protected traits from seemingly innocuous variables. An audit that examines only declared inputs to the pricing process will miss hidden bias, unless proxy effects are explicitly checked for. Proxy-discrimination metrics reveal why price disparities arise, by pinpointing variables that act as stand-ins for banned traits, giving supervisors and firms a lever to adjust, re-weight, or remove those inputs. Eliminating proxy effects does not force insurers to ignore genuine risk factors; but requires that their influence be justified on its own predictive merit and not on covert correlations. This preserves the actuarial principle of pricing commensurate with risk. Proxy discrimination relates to the role of protected characteristics in the way that prices are calculated, while group fairness notions (reflecting the joint statistical behaviour of policyholder characteristics and prices) relate to the outcome of that process. The measures discussed in Annex I are not suitable for monitoring proxy discrimination. If this legislation will apply to insurance pricing, it should be highlighted how this law connects to already existing EU-law on discrimination in insurance. Insurers are already prohibited from using protected characteristics directly under the Gender Goods-and-Services Directive 2004/113/EC and the related Test-Achats judgment, which requires unisex premiums, as well as the Racial Equality Directive 2000/43/EC, both of which implement Articles 21 and 23 of the EU Charter. At the supervisory level, EIOPA's 2023 Supervisory Statement on Differential Pricing Practices (BoS-23-076) instructs undertakings to prevent unfair price-walking and indirect discrimination, through the Product Oversight and Governance (POG) process. The new proposed AI framework therefore should ideally be presented not as a new layer of fairness in isolation but as a focused instrument that operationalises existing obligations: in our view, it should require proxy-discrimination tests and model-governance processes that give supervisors evidence that pricing algorithms comply with regulations mentioned above. Literature: - Lindholm et al. (2022, Discrimination-free insurance pricing. ASTIN Bulletin) define proxy discrimination in the context of insurance pricing and propose price adjustments. - Lindholm et al. (2024, A multi-task network approach for calculating discrimination-free insurance prices. European Actuarial Journal), based on a motor insurance case study, demonstrate that proxy discrimination (in relation to ethnicity) can have a material impact on	Annex, they may vary from one use of AI systems to another. A reference to actuarial fairness has also been added.

		insurance prices. - Lindholm et al. (2024, What is fair? Proxy discrimination vs. demographic disparities in insurance pricing. Scandinavian Actuarial Journal) demonstrate that avoiding proxy discrimination and addressing group fairness notions are generally conflicting aims. Price adjustments to address group fairness can introduce new forms of discrimination. Requiring adherence of insurance prices to group fairness criteria would lead to arbitrary adjustments driven by the composition of an insurer's portfolio, which would introduce price distortions. Hence, criteria formulated in Annex I may be practically inapplicable (or potentially damaging if applied) in an insurance system. - We do not discount the societal value of group fairness or that substantial demographic disparities in insurance prices can be problematic. We suggest caution in adopting group fairness criteria as decision objectives and advise that addressing direct and proxy discrimination take precedence. There is a need for trade-offs and for quantitative metrics of proxy discrimination to be added to the regulatory toolbox. - Lindholm et al. (2024, Sensitivity-Based Measures of Discrimination in Insurance Pricing. SSRN) introduce such measures and demonstrate their usefulness for identifying and quantifying discriminatory effects.	
113	Gesamtverband der Deutschen Versicherungswirtschaft	The statements in the 'Fairness and ethics' section can be misunderstood as an extension of the requirements in Art. 6 ff. AI Act. Thematically, they are of secondary importance in the risk management of companies. It would be necessary to delete them. Furthermore, 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 is questionable. We suggest a deletion.	Noted. The Opinion is consistent with the underlying principles of sectoral legislation and no regulatory gaps have been identified. The Opinion acknowledges that different uses of AI systems may require different fairness metrics and has clarified that the examples included in Annex I are not meant to be prescriptive guidance.
114	CNP Assurances	The approach here is also too general and generic. CNP Insurance would like to further clarify expectations regarding bias in data and outputs to	Noted. The Opinion clarifies that undertakings should make reasonable

		account for practical limitations and to align definitions of fairness with existing regulatory and actuarial frameworks. In addition, assigning clear organizational responsibility for ethical risks and broadening guidance on hidden biases, redress mechanisms, and monitoring models would enhance the practical usefulness of the advice. Regarding the definition of equity itself, there are various and occasionally conflicting definitions (e.g., equal opportunities and demographic parity). It is necessary to clarify the interpretation expected from the commitments applied, to promote regulatory uniformity within companies. Regarding point 3.12, the "consumer-centric" approach is not very clear and seems difficult to enforce in practice when companies rely on externally developed AI tools, such as general-purpose chatbots. In such cases, we suggest that customer centricity be interpreted as a responsibility to assess and manage the risks involved in using these tools rather than ensuring full control In addition, it seems desirable to indicate that the "corporate culture" must be materialized by clear policies and procedures, adapted governance with formalized opinions of experts for the examination of AI projects sent to the highest level of the organization for decision, and regular training on the existence of these procedures and committees. Section 3.13 currently states that they must be "free from bias". While this is an important objective, insurers should be required to demonstrate that they have taken reasonable steps to identify and mitigate bias, including through model correction techniques. This reflects the fact that some biases may be unknown or unavoidable, especially in third-party AI systems or those trained on large-scale internet datasets. Regarding point 3.15, we ask for more details on the means of appeal.	efforts to remove biases in the data, including potential unlawful proxy discriminatory variables. The Opinion acknowledges that the approach to AI systems should also include frameworks where the roles and responsibilities of different staff and the interplay between them are clearly defined. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring. Regarding redress mechanisms, the Opinion now refers to redress mechanisms (e.g. complaints resolution processes) which can be used by customers when they have been harmed by

			the use of an AI system in insurance.
115	IRSG	The principle of pursuing the best interest of the customer, as referenced by EIOPA in section 3.12 and derived from the IDD framework, is particularly relevant and appropriate for AI systems that have a significant impact on customers. However, its application does not appear relevant in cases where AI systems are used exclusively for internal purposes, with no direct or indirect effect on end customers. We encourage EIOPA to clarify its position on this matter. Additionally, we note that the data quality requirements outlined in section 3.13 are quite far-reaching. While data quality is important, the related requirements should be applied proportionally, taking into account the level of impact that an AI system has on the company and its customers. The same reasoning applies to fairness and non-discrimination metrics and redress mechanisms, as outlined in paragraphs 3.14 and 3.15. A one-size-fits-all approach could impose unnecessary constraints on low-risk AI applications, potentially hindering innovation without a corresponding benefit in terms of fairness and ethics. Special mention should be made of the requirement for the data to be free of bias (sections 3.13 and 3.18), because it may not be possible for firms to make use of data sets that are completely “free from bias”: the structured data that firms use depends on underlying data concepts (e.g: premiums, claims, settlements, policy data, policyholders) and there may be some implied biases in that underlying data. Firms apply data governance principles to data concepts, including ensuring data accuracy and completeness, to mitigate biases related to data collection and recording. But, depending on how “bias” is defined, it may not be realistic to suggest that firms can completely eliminate bias. We therefore propose that EIOPA explains more clearly how it understands the term “bias” and what it means for data to be “free from bias” in an AI context. We further recommend that EIOPA qualifies its guidance with a proportionality requirement to the effect that, while undertakings should do what they can to understand, put guardrails around, and mitigate bias (and document their efforts to do so), regulators should recognise that it may not be possible for firms to completely eliminate bias. One last consideration we would like to point out is related to price discrimination. It is important to distinguish between "discrimination" and "differentiation", a core principle of the insurance industry. Indeed, "differentiation" involves setting premiums based on the level of risk each policyholder presents. A crucial aspect of this practice is actuarial fairness, which ensures that individuals with the same risk profile pay the same amount. It is well known that	Noted. The Opinion recognises that governance and risk management of AI systems should be proportionate to their use, which for instance would enable placing less emphasis on fairness and ethics for systems that don't affect customers directly. Concerning biases in the data, while noting that certain variables need to be used to underwrite risks in insurance, the Opinion clarifies that undertakings should make reasonable efforts to remove biases in the data, including potential unlawful proxy discriminatory variables. Regarding redress mechanisms, the Opinion clarifies that they do not need to be specific to AI systems; complaints mechanisms that undertakings already have in place would normally suffice to enable customers to seek redress when they have been harmed by the use of an AI system in

		the application of AI has facilitated a greater determination of the risk involved for each person seeking insurance. As long as this is done, this is legitimate, even if it means that more people are left uninsured or are required to pay a higher premium than before this level of precision was achieved. On the contrary, "discrimination" occurs when differentiation is based on factors prohibited by law, like gender in the EU (and others at a national level), or whenever factors that are not causally related (or not having a strong link correlation) to the specific risk covered are used as risk factors (see EIOPA, “Artificial Intelligence…”, 2021, pp. 33 ss.). That is, for example, credit rating of the potential insured should not be used to set the premium for car insurance, as it does not affect the driving risk at all, but it could be used, in principle, for credit insurance. In conclusion, there are factors that cannot be taken into account in calculating the premium, such as gender, because they are prohibited by a legal provision. But this does not mean that all other risk factors can be used legitimately without further ado, because they can only be used if they have a causal relationship (or a strong correlation link) with the specific risk to be covered. This, of course, has to be assessed on a case-by-case basis. To enhance clarity, we suggest adding the following phrase to sect. 3.13 “However, the principle of fairness should be applied in a manner that distinguishes between unjustified discrimination and legitimate risk differentiation. Where differentiation is based on objective, actuarially sound, and legally permissible factors it should not be considered biased”. Finally, the sect. 3.15 states the convenience of putting in place redress mechanisms to enable customers to access and seek redress when they have been negatively affected by an AI system. The IRSG wonders whether it would not be consistent with that provision for insurance undertakings to inform customers in advance about whether a certain AI system is used for the product they are interested in taking out, for what purpose it is used and to what extent it may adversely affect them.	insurance. Furthermore, as explained in the transparency and explainability section, the explanations should be adapted to the needs of different recipient stakeholders.
117	CRO Forum	This section focuses largely on an insurance firm’s customers. Fairness to employees and other stakeholders may also need to be considered in this section. We support the connection drawn between a firm’s wider fairness and ethics approaches/policy and responsible use of AI Systems. In paragraph 3.13, the assertion on data completeness, bias-free and accuracy for training models may become outdated especially if firms obtain ‘off-the-shelf’ AI systems from	Noted. EIOPA has focused on key principles and requirement in insurance legislation that are relevant for the use of AI systems, and not on other aspects that might be more relevant for social and labour law.

		vendors, where the completeness of the training data set may not be clear to the user. While GenAI based systems can't invent new data, they do produce unique outputs that weren't explicitly in its training data, which over time feed into the training data of future AI systems. The focus on training set in this section, could also be supplemented to encourage awareness and proportional and risk-based management of model drift and data poisoning. Firms will need to make and record their choices about what is considered to be fair and how that links to a firm's culture and risk appetite. These choices and decisions need to be clearly justified and documented to be able to explain these at a later time and actively revisited as perception, culture and expectations change. We support the emphasis placed on the need for a proportional and risk-based approach, ensuring proportional management of fairness and bias risk. For more material AI Systems with a high degree of impact on customer outcomes, use of fairness and non-discrimination metrics may be needed including the use of proportional fairness assurance. As public perceptions evolve routine checks on what constitutes fair and ethical AI use could also be considered.	Nevertheless, the Opinion acknowledges the importance of social dialogue and has explicitly mentioned this possibility in the text of the Human Oversight section. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring. A reference to model drift has been added to the accuracy, robustness and cybersecurity section of the Opinion. Regarding the documentation of choices, the Opinion also states that following a risk-based and proportionate approach, undertakings should keep appropriate records of the training and testing data and the modelling methodologies to enable

			their reproducibility and traceability.
118	European Financial Congress	The opinion rightly points to the need to use AI fairly and ethically, avoid discrimination and ensure transparency. However, implementing sophisticated ethical and anti-bias controls can be costly and technically difficult, especially for complex models. It is worth considering limiting the requirements to cases where the risk of discrimination is real. In addition, while fully supporting the general principles of fairness, ethics and avoidance of discrimination, it is important to take into account the specifics of the insurance business, where differentiating customers on the basis of characteristics significantly correlated with risk is fundamental to proper risk assessment and product pricing. In this regard, EIOPA in its opinion of 2023 rightly emphasizes that not every differentiation constitutes discrimination. Thus, in the context of the proposed redress mechanisms, the opinion should clearly distinguish legitimate risk differentiation from unjustified discrimination. It should also be noted that the introduction of a broad, easily accessible customer redress mechanism in the context of AI decisions carries serious risks to the competitiveness and innovation of the insurance industry. Among these risks are: a) Increase in complaints and disputes - Easy access to an appeals mechanism can lead to mass complaints, including cases where AI decisions are in accordance with the law and best practice. - An increase in the number of appeals means that additional resources (personnel, support systems) need to be deployed, which increases operational costs. b) Risk of being overly cautious and limiting innovation - Companies may limit the use of modern, complex AI models (e.g., machine learning), which are more difficult to explain, in favor of simpler, less effective solutions to minimize the risk of disputes. (c) Risk of ambiguity and regulatory arbitrage	Noted. As explained in the Impact Assessment, the Opinion is based on existing provisions and principles in insurance legislation, which should limit the compliance costs for undertakings. For example, in the specific case of redress mechanisms mentioned in the comment, the Opinion has clarified that redress mechanisms do not need to be specific to AI systems; complaints mechanisms that undertakings already have in place would normally suffice to enable customers to seek redress when they have been harmed by the use of an AI system in insurance.

		- The lack of precise guidance on when an AI decision can be considered “inappropriate” or “discriminatory” leads to legal uncertainty and the risk of divergent interpretations by courts and regulators. - This may result in differences in market practice across EU countries. (d) Compliance and implementation costs - The need to ensure full auditability, explainability and human intervention for any AI system generates high implementation and maintenance costs. - Particularly acute for smaller entities that do not have extensive legal and IT departments. (e) Reputational risk - Public disputes over AI decisions can lead to a loss of customer confidence in the industry as a whole. Accordingly: - The appeal mechanism should be proportionate to the risk and importance of the decision. - Clear guidelines are needed on when and to what extent a customer can successfully challenge an AI decision, and when differentiation is justified.	
119	European Confederation of Institutes of Internal Auditing	-The guideline should describe the level of oversight be required for autonomous systems and for third-party "black box" type models, the expected controls should be defined. -Training data should be timely to prevent model drift, and control needs to be monitored throughout the model's lifecycle.Audit should follow the proportionality principle in this context. -The outcomes of AI systems should also be regularly monitored and audited, including with the use of fairness and non-discrimination metrics (see examples of metrics for high-risk AI systems in Annex I). To be clarified if “audited” (3.14) refers to Internal Audit activities of other audit/control activities performed by other functions. If it refers to Internal Audit, it should be clarified/introduced the risk-based approach principle, to avoid defining a pre-defined frequency for Internal Audit activities on AI.	Noted. Concerning third party black-boxes, the Opinion clarifies that undertakings are responsible for the AI systems they use, even if provided by third parties, and should take steps such as contract clauses, audits, and monitoring to ensure proper governance and risk management.

			Moreover, a reference to model drift has been added to the accuracy, robustness and cybersecurity section of the Opinion. Regarding the reference to internal audit vs. external audit, this has not been specified in the Opinion in view of its principle-based approach. However, the Opinion indeed explains that the risk-based and proportionality principle is applicable to all the governance and risk management measures described in the Opinion.
120	Federation of European Risk Management Associations (FERMA)	FERMA fully support the adoption of a customer-centric approach by insurance undertakings. However, it must be stressed that the effectiveness of redress mechanisms rely on the ability of (corporate) customers to discern whether an AI system was the cause of a negative impact they suffered in the first place. Insurance undertakings should therefore make sure to inform their customer when an AI system is used as a part of a product or a service, what the purpose of said AI system is, and how it may influence outcomes affecting the interests of the customer. AI implementation requires an analysis of its intervention areas, decision influence, and sustainability factors to ensure it adds value to both organizations and customers while maintaining service quality. Moreover, we recommend that undertakings follow internationally recognised standards, such as the UNESCO's Recommendation on the Ethics of Artificial Intelligence, to facilitate the ethical use of AI systems.	Noted. Regarding redress mechanisms, the Opinion clarifies that they do not need to be specific to AI systems; complaints mechanisms that undertakings already have in place would normally suffice to enable customers to seek redress when they have been harmed by the use of an AI system in insurance. Furthermore, as explained in the

			transparency and explainability section, the explanations should be adapted to the needs of different recipient stakeholders.
121	BETTER FINANCE	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.	Noted. See reply to the previous comment regarding redress mechanisms and information to be provided to customers.
122	Actuarial Association of Europe	Key message: The AAE supports the inclusion of fairness and ethics within the Opinion. We suggest refining the expectations around bias in data and outputs to reflect practical limitations and aligning definitions of fairness with existing regulatory and actuarial frameworks. Additionally, assigning clear organisational accountability for ethics-related risks and expanding guidance on hidden biases, redress mechanisms, and model monitoring would enhance the Opinion’s practical utility. Detailed response: We welcome the strong focus on fairness and ethics in the Opinion. These principles are fundamental to public trust and align closely with actuarial values. We particularly endorse the need for explicit assignment of ethics risk at a senior level within the organisation. Without such clear accountability, there is a real danger that ethical issues could be	Noted. Concerning biases in the data, the Opinion clarifies that undertakings should make reasonable efforts to remove biases in the data, including potential unlawful proxy discriminatory variables. A reference to customer’s vulnerability has also been added in the risk-based and proportionality section and a cross-reference to the paragraph addressing

		overlooked despite Board-level awareness. With regard to training data, Section 3.13 currently states that it should be "free of bias". While this is an important goal, we believe it would be more practical to require insurers to demonstrate that they have taken reasonable steps to identify and mitigate bias, including through model correction techniques. This reflects the reality that some biases may be unknown or unavoidable, particularly in third-party AI systems or those trained on large-scale internet datasets. Hidden or indirect biases—such as those embedded in assumptions or proxies—also warrant further attention. We suggest that the Opinion explicitly call for the use of both pre- and post-modelling tests to assess fairness in outcomes, especially where AI decisions affect pricing, underwriting or claims. The lack of access to protected characteristics (e.g. race or gender) in datasets can make bias detection more difficult. In such cases, guidance on proxy testing or indirect fairness assessments would be welcome. On the definition of fairness itself, we note that multiple and sometimes conflicting definitions exist (e.g. equal opportunity vs. demographic parity). We recommend that EIOPA clarify which interpretation it expects undertakings to apply, to support regulatory consistency and comparability across firms Section 3.12 refers to a “consumer-centric” approach. Some of our members noted that this may be difficult to uphold in practice when firms rely on externally-developed AI tools, such as general-purpose chatbots. In such cases, we suggest that customer-centricity be interpreted as a responsibility to assess and manage the risks of using such tools rather than guaranteeing full control. Additionally, it would be helpful if the Opinion referenced customer vulnerability and financial literacy explicitly, as these are relevant factors in understanding fairness and ethical risks in customer interactions. We also encourage elaboration of Paragraph 3.15 on redress. While we support the principle of giving customers the right to information and contestation, the mechanism for redress may vary across the value chain and by the nature of the system. We suggest distinguishing between redress for customers and internal feedback mechanisms to support model retraining and correction. These serve different purposes but both are critical to trustworthy	the issue of third parties has also been added in the data governance section. Moreover, a reference to model drift has also been added to the accuracy, robustness and cybersecurity section of the Opinion. Concerning redress mechanisms, the Opinion has clarified that redress mechanisms do not need to be specific to AI systems; complaints mechanisms that undertakings already have in place would normally suffice to enable customers to seek redress when they have been harmed by the use of an AI system in insurance. The term “meaningfully explainable” is maintained since it is in line with the principles based approach of the Opinion as well as with other EU legislations (e.g. GDPR and AI Act).

		AI. A further enhancement would be to include a paragraph addressing model and system governance, including model drift, lifecycle testing, and performance monitoring. These are often underdeveloped in current insurance practices. Incorporating guidance on fairness metrics (e.g. F1-score, recall, precision), explainability, and robustness under a governance and testing umbrella would promote more reliable outcomes. Lastly, it may be helpful to clarify or reconsider terms such as "meaningfully explainable", which may be open to interpretation. Definitions grounded in technical standards would support more consistent application.	
123	Finance Watch	Given the complexity, autonomy and opacity of AI systems, there is a need for redress and liability rules tailored to the unique characteristics and challenges of AI to ensure that consumers are able to seek redress in cases where damages are caused by the use of AI by financial institutions. The existing EU regulatory regime (including the sectoral legislation covered by the EIOPA Opinion), however, does not contain any liability rules tailored to the deployment of AI in the financial sector, or in any other retail sector. Recognizing this important regulatory gap, in 2022, the European Commission proposed the introduction of a Directive on adapting non-contractual civil liability rules to artificial intelligence (AILD). This proposal had the aim to cover non-contractual civil liability for damages caused by an output of an AI system or by the failure to produce an output. Most importantly, the rules aimed at overcoming the challenges of the black-box nature of AI systems that make it difficult for consumers to bring a successful liability claim when opaque AI systems are involved by introducing a rebuttable 'presumption of causality'. This concept would ease the burden of proof for claimants, meaning that if a victim can show that someone was at fault for not complying with a certain obligation relevant to their harm, and that a causal link with the AI performance is reasonably likely, the court can presume that this non-compliance caused the damage. While this proposal went in the right direction of addressing an important consumer protection gap, in early 2025, the Commission unfortunately announced the withdrawal of the AILD. To ensure the adequate protection of consumers subjected to automated decisions made by AI systems deployed in the insurance sector, a new EU proposal to establish non-contractual civil liability rules for AI should be introduced. This new proposal, however, should not be a mere copy of the previous proposal but should introduce not merely, as in the last AILD proposal, an easing of the burden of proof but instead a reversal of the burden of proof in favour of the individual claimant. Under the previous proposal, consumers would	Noted. The Opinion states that the roles and responsibilities of different staff and the interplay between them should be clearly defined. EIOPA notes the status of the legislative process of the Directive on adapting non-contractual civil liability rules to artificial intelligence (AILD) and will continue to monitor further developments on this area.

		have to still resort to the disclosure of evidence to obtain relevant documentation that can eventually help them to prove fault of the AI operator. Consumers, however, may not have the expertise and sufficient skills to interpret this information, making it necessary to refer to external technical expertise which in turn could significantly increase the costs and the length of any court proceedings to bring a claim. Harmonized rules in this area are also needed to avoid legal uncertainty and the risk of increased costs for businesses. Several EU Member States are considering, or even concretely planning to introduce legislative measures on civil liability for AI. Therefore, a lack of EU-level rules will result in fragmentation and increased costs for businesses operating cross-border.	
124	Insurance and Pensions - Denmark	Is should be considered to clearly specify that the section on Fairness and Ethics is based on solely IDD and therefore only cover the scope of IDD i.e. systems directly affecting insurance distribution. (thus not cov-ering insurance models, claims handling etc.) This should be highlighted to clarify scope for this section and consider-ations outside scope of IDD should clearly be highlighted as optional. And in addition it is suggested to highlight the importance of propor-tionality and risk level in these considerations. Text specific comments: Point 3.12 (last part): “This includes developing a corporate culture that includes ethics and fairness guidance and relevant trainings.” Comment: While Article 17 of IDD mention fairness, it does not imply developing a corporate culture including guidance and training. This sentence should be removed. IDD art. 10 mentions requirements for training, but these are general requirements not targeted at fairness and ethics.	Noted. The Opinion has clarified that the scope of the insurance sector legislation mentioned therein is not altered, and the principles outlined in the Opinion are applicable to the use of AI systems in insurance within the scope of the Opinion, based on requirements in sectoral legislation, and following a risk based and proportionate approach. The Opinion also explains that the proportionality principle is applicable to all the governance and risk management measures described in the Opinion. Regarding the text specific comments, we believe that they are consistent with the

		Point 3.13: The text in 3.13 is in line with Solvency II, which is not referenced for this section. Consider moving the sentence to “Data governance” to differentiate the data-specific considerations from the additional considerations on ethics and fairness. Point 3.14: “The outcomes of AI systems should also be regularly mon-itored and audited, including with the use of fairness and non-discrimination metrics (see examples of metrics for high-risk AI sys-tems in Annex I).” Comment: Point 3.14 does in our opinion not follow from IDD; but “The outcomes of AI systems should also be regularly monitored and audited” can follow from Solvency II (which is not referenced for this section in 3.11). Use of fairness metrics and non-discrimination metrics can follow from IDD but only for systems directly affecting insurance distribution. This should be highlighted to clarify scope and it could be considered to add “where relevant” in the sentence. Point 3.15: “Adequate redress mechanisms should also be in place to enable customers to access and seek redress when they have been neg-atively affected by an AI system.” Comment: The wording in point 3.15 should be clearly labeled as only related to insurance products according to the scope of the IDD. That ‘redress mechanisms should be in place’ cannot be formulated as a broad requirement for all AI systems.	underlying principles of sectorial legislation. Regarding the redress mechanisms, the Opinion has clarified that redress mechanisms do not need to be specific to AI systems; complaints mechanisms that undertakings already have in place would normally suffice to enable customers to seek redress when they have been harmed by the use of an AI system in insurance.
125	Wind Tre S.p.A.	In addition to the measures outlined, it may be beneficial for regulatory authorities to provide a dedicated training program tailored specifically for AI systems interacting directly with customers. Such a program could be developed in collaboration with market operators to ensure that it reflects the practical realities and challenges faced by the industry. This initiative would not only help create a consistent customer-centric approach across the sector but also serve as an anti-competitive distortion mechanism, fostering a level playing field. By engaging market stakeholders in the design and implementation of the training program, it	Noted. EIOPA aims to continue collaborating with stakeholders to monitor market developments and provided further guidance, where appropriate.

		would ensure alignment with best practices and enhance the responsible and ethical use of AI systems. Moreover, such a program could contribute to ensuring a homogeneous customer-centric approach, reinforcing trust and transparency across all market players, while enabling regulatory authorities to establish clear guidance and standards. This collaborative effort would ultimately strengthen consumer protection and promote innovation in an ethically responsible manner. Also in this case, it is necessary to describe in more detail the commitments that weigh on providers of AI systems from those that weigh on deployers, so as to allow the appropriate fairness interventions to be carried out by the correct entity that must put them into practice.	Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring.
127	ANASF	We agree with EIOPA's comments regarding the fairness of AI systems and ethics, and the provision of adequate redress mechanisms to enable customers to seek compensation if they have been harmed. It is important that firms are aware that they will be responsible for the AI systems they implement.	Noted.
129	BEUC - The European Consumer Organisation	- Title: In line with the principles included in the report of EIOPA's Consultative Expert Group on digital ethics in insurance , BEUC recommends changing the title to "Fairness and non-discrimination" and adding a point on the topic of non-discrimination which does not gain any attention so far. - Point 3.11: BEUC recommends referencing in addition the report from EIOPA's Consultative Expert Group on Digital Ethics in insurance as the report provides valuable guidance, notably on pricing. - Point 3.12: There are wide divergences as regards the interpretation of treating customers "fairly and according to their best interest". BEUC recommends introducing additional criteria to ensure regulatory convergence at a high level of consumer protection. - Point 3.15: It should be clarified that adequate redress mechanisms in line with the ADR Directive to offer "independent, impartial, transparent, effective, fast and fair alternative dispute resolution procedures." Currently, ADR bodies in the insurance sector are often set up by the business association representing insurance operators which do not offer an independent outcome.	Noted. The title of this section has not been modified, and the Opinion includes explicit references to non-discrimination and bias, both in the text of the Opinion as well as in the Annex. The report from EIOPA's Consultative Expert Group on Digital Ethics in insurance is mentioned in footnote 8 of the Opinion, and more prominently in the Annex. The Opinion is kept principle-based, with some specific and non-prescriptive examples

			included in the Annex. More detailed guidance may be developed in the future, where appropriate. Regarding the redress mechanisms, the Opinion has clarified that redress mechanisms do not need to be specific to AI systems; complaints mechanisms that undertakings already have in place would normally suffice to enable customers to seek redress when they have been harmed by the use of an AI system in insurance
130	Spanish Association of Risk Management and Insurance, known as AGERS	The areas in which it intervenes must be analysed, as well as the degree of influence on decisions, the factors that are taken into consideration, especially those relating to sustainability, and the aforementioned influence on the quality of service provision. It must be ensured that AI adds value not only to organisations in the sector but also to customers.	Noted.
131	AI & Partners	The focus on fairness and ethics is crucial for ensuring consumer trust in AI-driven insurance. However, the Opinion could benefit from more concrete methodologies for detecting and mitigating bias in AI models. The introduction of standardized fairness metrics—such as demographic parity or equalized odds—would enhance accountability. Additionally, establishing independent fairness audits and external review mechanisms could provide further safeguards. The Opinion should also emphasize consumer education initiatives, ensuring policyholders understand how AI-driven decisions impact them and how they can challenge unfair outcomes. Strengthening guidance on ethical AI decision-making frameworks would also support industry alignment.	Noted. The Opinion is kept principle-based, with some specific and non-prescriptive examples of fairness metrics included in the Annex. More detailed guidance may be developed in the future, where appropriate. The Opinion does not explicitly promote consumer education initiatives, but it states that explanations should also be adapted to

			the needs of different recipient stakeholders.
		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?	
132	BIPAR	As done in other sections and for the sake of clarity, we believe that it would be useful to refer in this section to the taking into account of risk-based and proportionality considerations. Here a more proportionate approach could ensure for example that data governance expectations are less ambitious for AI systems that have little or no impact on customers.	Noted. The Opinion explains that the proportionality principle is applicable to all the governance and risk management measures described in the Opinion.
133	Studio legale Floreani	A consistent and accountable data governance framework is essential for trustworthy AI deployment in the insurance sector. The current Opinion would benefit from additional safeguards ensuring traceability, quality, and lawful processing of personal and operational data shared between insurance undertakings and distributors. In accordance with GDPR, joint controllership arrangements and processor obligations must be clearly defined, especially when AI training data or outputs are shared. Proposals include: Establishment of protocols for the vetting and supervision of third-party data providers. Introduction of contractual safeguards to prevent bias in data collection and use. Development of minimum quality standards for training datasets. Consideration of a centralised registry of data flows and provider certifications.	Noted. The Opinion is kept principle-based, with some specific and non-prescriptive examples included in the Annex. More detailed guidance may be developed in the future, where appropriate.
134	AFPA, Austrian Financial & Insurance Professionals Association	Gute Datenqualität ist entscheidend. Anforderungen sollten auf bestehende Datenschutzprozesse aufbauen und proportional umsetzbar sein. Im Bereich der Datenverwaltung stellt sich vor Allem die Frage nach der Harmonisierung mit den geltenden Datenschutzgesetzen. Wir alle kennen die Problematik mit dem Datentransfer in und aus den USA. Das aktuell in Geltung stehende EU-US Privacy Framework in Kombination mit der Zertifizierung der teilnehmenden US-Unternehmen gleicht eher einem „Feigenblatt“ als einer fundierten Lösung. Durch die vielfach unberechenbaren Aktivitäten der	Noted.

		aktuelle US-Regierung werden Stimmen lauter, dass hier an der Aufrechterhaltung einer einvernehmlichen Lösung wenig Interesse besteht. Mit Zerfall dieser Lösung, stehen EU-Unternehmen im Zusammenhang mit KI-Systemen und der damit verbundenen Offenlegungsverpflichtung in einer unlösbaren Situation. Europa muss hier noch höher Anstrengungen unternehmen, um der US-Umklammerung zu entkommen. Hier ist auch das europäische Gießkannen-Fördersystem „zu Grabe zu tragen“, da dies ein Relikt aus vergangenen Zeiten darstellt. Wenn wir uns hier emanzipieren wollen, muss „am großen Rad gedreht werden“, und nicht nur kosmetische Änderungen im Mittelpunkt der Bestrebungen stehen. Versäumnisse bei einer eigenen Ratingagentur, IT-Systemanbietern bis hin zur KI-Entwicklung müssen der Vergangenheit angehören. Politisch bewegen wir uns global weg vom Recht des Gesetzes hin zum Gesetz des Stärkeren. Diese bedenkliche Entwicklung kann nur durch den Aufbau von Gegenpolen bewältigt werden. Europa benötigt nicht nur „regulations“, sondern eine Struktur, die uns wieder wettbewerbsfähig macht. Good data quality is crucial. Requirements should build on existing data protection processes and be proportionally implementable. In the area of data management, the question of harmonization with existing data protection laws arises. We all know the issues with data transfer to and from the USA. The current EU-US Privacy Framework, combined with the certification of participating US companies, resembles more of a "fig leaf" than a solid solution. Due to the often unpredictable activities of the current US government, voices are growing louder that there is little interest in maintaining a consensual solution. With the collapse of this solution, EU companies are in an unsolvable situation regarding AI systems and the associated disclosure obligations. Europe must make even greater efforts to escape the US grip. The European "watering can" funding system must also be laid to rest, as it is a relic of the past. If we want to emancipate ourselves here, we must "turn the big wheel" and not focus only on cosmetic changes. Failures in establishing our own rating agency, IT system providers, and AI development must be a thing of the past. Politically, we are moving globally from the rule of law to the law of the strongest. This worrying development can only be countered by building counterweights. Europe needs not only "regulations" but a structure that makes us competitive again.	
136	Insurance Europe	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.	Noted. The Opinion has clarified that the scope of the insurance sector legislation mentioned therein is not altered, and

			the principles outlined in the Opinion are applicable to the use of AI systems in insurance within the scope of the Opinion, based on requirements in sectoral legislation, and following a risk based and proportionate approach.
138	Lloyd's Market Association	We agree that entities should ensure that the data used to train the AI is complete, accurate and appropriate. However, we would challenge the words in parentheses following each of the words "complete", "accurate" and "appropriate" – this carries the risk of defining these terms. We do not believe this is helpful and is not done anywhere else in the Opinion. By way of example of the dangers of such as approach, we note the "definition" of "accurate" as being "no material errors and free of bias". An unqualified requirement to ensure that a data set is unbiased is likely to be often unachievable from a review of the data set itself because any bias may be detectable only in aggregate outcomes or through iterative model monitoring. This applies equally to data collected by the undertaking and third party data sets. Furthermore, data is inherently biased. Any assessment of training data must distinguish correlation from causation. Protected characteristics may correlate with legitimate risk factors (e.g. population density and socio-economic profile). Risk-pricing variables therefore differentiate by design and can appear biased unless their explanatory link to claims outcomes is demonstrable. What is important is that the data does not lead to unlawful discrimination. Accordingly, undertakings may only ever be able to take a best endeavours approach to ensuring that data sets are unbiased (without considering outcomes) and the current framing of "accurate" does not acknowledge that reality. We note, in this regard, paragraph 3.33 imposing a standard of proportionality as to the accuracy of the AI system and we believe this yardstick can be similarly applied to the accuracy of data sets. We do not believe the intent was to introduce definitions to these words, but we think that the Opinion should be divested of the words in the parentheses.	Noted. In line with the principle based approach of the Opinion, we have softened the definitions of "complete", "accurate" and "appropriate" by including purely illustrative examples. Moreover, while noting that certain variables need to be used to underwrite risks in insurance, the Opinion clarifies that undertakings should make reasonable efforts to remove biases in the data, including potential unlawful proxy discriminatory variables.
139	Dr. Paul Larsen	The wording in 3.18 seems to lack technical nuance present elsewhere in the document, as well as in existing regulation. The concern is that 3.18 sets an in-practice difficult if not	Noted. The Opinion has been amended

		impossible standard of total completeness, accuracy, and appropriateness. In contrast, the risk-based approach reflected in 3.16 for data governance allows for less than perfect data governance standards for AI systems of minimal risk, which also matches the EU AI Act's approach. The same holds for 3.22 regarding documentation and record-keeping, and 3.30 regarding accuracy and robustness. The 2015/35 Solvency II document, Article 19 on the matter of data quality for the solvency-relevant matter of technical provisions sets high standards of data governance for what I consider a high-risk area (with respect to financial stability), yet also acknowledges options when such high standards are not met (Article 20).	acknowledging possible limitations in the data, which should be duly documented and addressed.
140	European Federation of Financial Advisers and Financial Intermediaries (FECIF)	We agree that it is necessary to implement a data governance policy that complies with applicable data protection legislation, even if this entails a cost for the company to verify the standard that the data must meet. We also believe that the required standard should be certified: certification will ensure that the data used meets the standard prescribed by the legislation, especially if the company uses external data acquired from a third party.	Noted. The Opinion is kept principle-based. More detailed guidance may be developed in the future, where appropriate.
141	AMICE	We would like to point out that extending data quality rules under Solvency II beyond their original scope to cover all AI applications should only occur with a clear legislative basis, avoiding regulatory overreach. Additionally, data governance expectation should be proportionate and scaled according to the specific risks and impact of each AI system. Moreover, when using AI systems developed by third parties, insurers remain accountable but may not have full access to training data and, thus, should be allowed to reasonably rely on quality assurances made by the third parties/developer.	Noted. The Opinion has clarified that the scope of the insurance sector legislation mentioned therein is not altered, and the principles outlined in the Opinion are applicable to the use of AI systems in insurance within the scope of the Opinion, based on requirements in sectoral legislation, and following a risk based and proportionate approach. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems they use, even if provided by third parties, and should take steps to

			ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring.
142	Institute of International Finance	As a general comment, EIOPA should limit the data governance discussion to the areas of underwriting, reserving, and technical provisions, which are explicitly referred to in those legislative acts that are cited in para. 3.16 as the legal basis. The requirement for 'a data governance policy which is aligned with the potential impact of the AI use case at hand' (para 3.17) lacks clarity on what alignment means in practice. 'Proportionate to' would be clearer language. Para 3.18 of the Opinion states that '[d]ata governance should ensure that the data used to train and test the AI system is complete …, accurate … and appropriate (consistent with the purposes for which it is to be used.' It also states that 'the undertaking should assess potential biases in the data and correct them in line with the undertaking's policy.' This creates a new standard rather than merely guidance, consistent with a pattern of imposing quasi-requirements via an Opinion. We oppose the introduction of quasi-requirements in this way. Furthermore, EIOPA should adopt a more flexible approach, scaling data governance expectations based on an AI system's impact on customers and on the insurance undertaking's business. In any case, the statement that 'the undertaking should assess potential biases in the data and correct them' (page 9) should specify 'actual biases' rather than potential ones. The important societal role of insurance undertakings in risk analysis of potential insureds means it is very important that obligations relating to bias are not imposed that go beyond existing applicable law. To do so may interfere with insurance undertakings' ability to engage in risk-based pricing. The expectation that 'the same data quality standards should apply' for external data acquired from third parties (para 3.20) may be very challenging to implement given market realities, even if it represents good practice, unless the Opinion also addresses the issue raised above about financial firms reporting difficulties in obtaining information from third parties about their AI technology.	Noted. The Opinion has clarified that the scope of the insurance sector legislation mentioned therein is not altered, and the principles outlined in the Opinion are applicable to the use of AI systems in insurance within the scope of the Opinion, based on requirements in sectoral legislation, and following a risk based and proportionate approach. The Opinion has been amended acknowledging possible limitations in the data, which should be duly documented and addressed, and highlights that undertakings should make reasonable efforts to remove biases in the data. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems and data they use, even if provided by third parties, and should take

		It is suggested the Opinion recognize the iterative nature of ML model development by encouraging phased implementation of data governance controls proportionate to a model's stage of development and materiality. An insurance company may deploy an AI system developed by a third party. As noted above, in this instance, the insurance company may not always have access to the dataset used for training the AI system and, therefore, the direct verification of data quality standards may not be practicable; the Opinion should clarify that insurance undertakings should be able to rely on the contractual assurances and independent validation reports provided by the third-party developer in such cases.	steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring.
143	Gesamtverband der Deutschen Versicherungswirtschaft	The data governance section indicates an orientation towards the requirements of Art. 10 of the AI Act on 'data and data governance', which applies exclusively to high-risk AI systems. Therefore, it should be made clear that the EIOPA opinion does not intend to extend these requirements to non-high-risk AI systems 'through the back door'. This would impose a considerable burden on insurance companies.	Noted. This Opinion does not set out new requirements and does not seek to alter the scope of the AI Act by extending the requirements of the AI Act for high-risk AI systems to all AI systems used in insurance.
144	CNP Assurances	CNP Assurances asks for clarification of expectations for bias, accuracy and completeness, especially in cases involving third-party data. Greater consistency in the terminology and scope of the opinion, as well as consideration of the broader data life cycle, would enhance the practicality and coherence of this section. The treatment of bias in this section would benefit from clarification. Paragraph 3.18 refers to the assessment and correction of biases, which seems to contrast with previous suggestions that the data should be entirely free of bias. In practice, biases are often unavoidable, especially in historical or third-party datasets. More consistent and pragmatic expectations, focused on reasonable mitigation efforts rather than elimination, would reflect operational realities and support achievable implementation. CNP Assurances suggests adding the mention that the creation of training datasets must comply with the principles of the GDPR in line with the doctrine of the national or European regulators concerned, e.g. CNIL (minimisation, legal basis, information of individuals, compatibility tests with the initial purposes of the processing).	Noted. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems and data they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring. The Opinion has been amended acknowledging possible limitations in the data, which should be duly

		Expectations regarding third-party data sources should also be strengthened. Insurers may not have full transparency or control over how this data is collected or processed. Paragraph 3.20 could be supplemented to reflect the need for consistent disclosure obligations and due diligence when working with external vendors. Finally, we also propose to expand the scope of the data quality section to reflect the full data lifecycle. Areas such as data collection (e.g., via LLMs or web scraping), feature engineering, and data enrichment can significantly influence model results and should be considered as part of effective AI governance.	documented and addressed, and highlights that undertakings should make reasonable efforts to remove biases in the data. The Opinion recognises that sound data governance should be applied throughout the AI system life cycle for data collection, data processing and post processing.
145	IRSG	We agree that sound data governance is fundamental to the safe and effective deployment of AI systems in insurance. However, it is worth noting that the legislative provisions of Solvency II and its Delegated Regulation, referenced in the Opinion as legal basis for data governance expectations, only relate to data quality in underwriting, reserving, and technical provisions. They do not impose specific and strict data governance obligations for other purposes, such as fraud detection, customer service automation, or marketing analytics. We therefore caution against any implicit expansion of these requirements into areas not covered by the legislative framework without a clear legislative mandate. The principles outlined by EIOPA in 3.18 could distinguish among AI systems based on the potential impact of these applications, calling for more stringent data governance to be applied to high-impact AI systems. This would align with the principle of proportionality, preventing unnecessary regulatory burdens on low-risk AI applications while maintaining effective oversight where needed. To address this, we recommend implementing the following amendments to sect. 3.18: “Data governance should ensure that the data used to train and test AI systems is complete (representative of the relevant population and sufficient historical information), accurate (no material errors and free of bias), and appropriate (consistent with its intended purpose). The scope and stringency of data governance measures should be proportionate to the AI system’s impact, with enhanced oversight required for high-impact AI applications, such as those used in underwriting, pricing, and claims handling, while lower-risk AI applications may be subject to lighter governance expectations. In particular, undertakings should assess potential risks related to data quality and fairness in AI-driven decisions and address them in line with their risk management policies. This should not prevent legitimate and actuarially justified risk differentiation, where permitted by applicable law”.	Noted. The Opinion has clarified that the scope of the insurance sector legislation mentioned therein is not altered, and the principles outlined in the Opinion are applicable to the use of AI systems in insurance within the scope of the Opinion, based on requirements in sectoral legislation, and following a risk based and proportionate approach. The Opinion explains that the proportionality principle is applicable to all the governance and risk management measures described in the Opinion, including the data governance section.

		Second, we note that in section 3.20, EIOPA acknowledges the possibility that training data may be sourced externally, but it does not address the broader case where an AI system itself is developed by a third-party and then deployed by an insurance company. While it is reasonable to expect that companies remain accountable for the AI systems they use, in line with outsourcing principles set out by Solvency II, we recommend EIOPA to recognise that a deployer may not always have full access to the datasets used to train a AI system developed by third parties. In such cases, data quality requirements should apply primarily to AI developers, while insurance undertakings deploying those AI systems should be allowed to rely on contractual assurances and independent validation reports from third parties, rather than being required to revalidate data they cannot reasonably access or control. To address this, we recommend adding the following phrase to sect. 3.20 “However, where an AI system is developed externally, insurers may not always have full access to the training data or methodologies used by third-parties. In such cases, insurance undertakings should be allowed to rely on contractual assurances, independent validation report and compliance attestations from third-party providers”. Third, according to sect. 3.17, “Undertakings should implement a data governance policy which is aligned with the potential impact of the AI use case at hand on consumers or the undertaking and in compliance with applicable data protection legislation”. An explicit reference to the impact it may have on the company's employees is missing. Any use of AI for employee surveillance, performance evaluation, or recruitment should be negotiated with trade unions and comply with GDPR.	Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems and data they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring. Finally, the Opinion focuses on key principles and requirement in insurance legislation that are relevant for the use of AI systems, and not on other aspects that might be more relevant for social and labour law. Nevertheless, the Opinion acknowledges the importance of social dialogue and has explicitly mentioned this possibility in the text of the Human Oversight section.
146	CRO Forum	In paragraph 3.17 and 3.19 we would recommend the reiteration that the data governance approach for AI systems should be risk based and proportionate as well as compliant with applicable data protection legislation. In paragraph 3.18 the comments above for question 5 should also be considered recognising the challenges of understanding training data for ‘off-the-shelf’ AI systems.	Noted. The Opinion explains that the proportionality principle is applicable to all the governance and risk management measures described in the Opinion,

			including the data governance section. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems and data they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring.
147	European Financial Congress	EIOPA's opinion rightly emphasizes the need to ensure high quality, completeness and representativeness of data used in AI systems, especially when it affects customers or the operations of an insurance company. It is worth noting that the document extends the requirements under Solvency II - which have traditionally focused on actuarial and financial data (e.g., for calculating reserves) - to a broader range of data used in AI systems.	Noted. The Opinion has clarified that the scope of the insurance sector legislation mentioned therein is not altered, and the principles outlined in the Opinion are applicable to the use of AI systems in insurance within the scope of the Opinion, based on requirements in sectoral legislation, and following a risk based and proportionate approach.
148	European Confederation of Institutes of Internal Auditing	- The data quality should not be limited to reserve and underwriting	Noted. EIOPA agrees with this statement. For example, sound data governance is fundamental to ensuring that consumers are treated fairly,

149	Federation of European Risk Management Associations (FERMA)	Insurance undertakings should inform customers when their data is used to train an AI system – even when said data was initially collected for another purpose. Moreover, undertaking should inform customers of the purpose of the AI system trained using their data. Lastly, customers should have the possibility to opt out of having their data used to train an AI system, either partially or completely. Additionally, we emphasize that data governance should focus on data granularity, structure, algorithms, and input/output relationship; special care should be given to analysing potential bias patterns. Validation of external data sources should go through broader organizational approval forums, not just the AI implementation team, in order to ensure reliable, unbiased data sources through collaborative oversight.	Noted. While not going into such level of detail, in line with its principle-based approach the Opinion acknowledges that the explanations should be adapted to the needs of different recipient stakeholders. In addition, while noting that certain variables need to be used to underwrite risks in insurance, the Opinion clarifies that undertakings should make reasonable efforts to remove biases in the data, including potential unlawful proxy discriminatory variables.
150	BETTER FINANCE	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	Noted. The Opinion has been amended acknowledging possible limitations in the data, which should be duly documented and addressed, and highlights that undertakings should make reasonable efforts to remove biases in the data. The Opinion explains that the proportionality principle is applicable to all the governance and risk management measures described in the Opinion,

		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).	including the data governance section.
151	Actuarial Association of Europe	Key message: The AAE supports EIOPA's emphasis on high-quality data as foundational to the trustworthy use of AI systems. However, we suggest clarifying expectations around bias, accuracy, and completeness, particularly in cases involving third-party data. Greater consistency in terminology and scope across the Opinion, and consideration of the broader data lifecycle, would strengthen the practicality and coherence of this section. Detailed response: We welcome the focus on ensuring that data used to train and test AI systems is accurate, complete, appropriate, and relevant. However, we suggest clarifying that data should be "reasonably" complete and accurate, as full completeness may not be practical in many insurance applications, especially when unstructured or third-party data is involved. The treatment of bias across this section would benefit from further clarification. Paragraph 3.18 refers to the assessment and correction of bias, which seems to contrast with previous suggestions that data should be entirely free of bias (e.g., Paragraph 3.13). In practice, bias is often unavoidable, especially in historical or third-party datasets. A more consistent and pragmatic expectation—focusing on reasonable mitigation efforts rather than elimination—would reflect operational realities and support feasible implementation. Terminological consistency would also enhance the clarity of the Opinion. Paragraph 3.16 uses terms that differ from Paragraph 3.13 and from Article 82 of Solvency II. We suggest that EIOPA align the terminology used throughout the Opinion, or provide clarification on any	Noted. The Opinion has been amended acknowledging possible limitations in the data, which should be duly documented and addressed, and highlights that undertakings should make reasonable efforts to remove biases in the data. Moreover, the Opinion recognises that sound data governance should be applied throughout the AI system life cycle for data collection, data processing and post processing.

		intended distinctions. This would help users interpret requirements consistently. In addition, we propose that EIOPA consider the principles outlined in the European Standard of Actuarial Practice 1 (ESAP1), particularly those relating to data quality and reliance on third parties (Sections 3.5 and 3.3). These principles are well-established across the actuarial profession and may offer useful reference points for insurers when assessing the adequacy and governance of data. ESAP1: https://actuary.eu/wp-content/uploads/2019/10/ESAP1-Revised-11-10-2019-FINAL.pdf We further recommend strengthening expectations regarding third-party data sources. Insurers may not have full transparency or control over how such data is collected or processed. Paragraph 3.20 could be expanded to address the need for consistent disclosure obligations and due diligence when engaging with external providers. Lastly, we suggest broadening the scope of the data quality section to reflect the full data lifecycle. Areas such as data collection (e.g. via LLMs or web scraping), feature engineering, and data enrichment can significantly influence model outcomes and should be considered as part of effective AI governance. Including these dimensions would enhance the technical depth and practical applicability of this section.	
152	Finance Watch	To avoid the risks outlined in our answer to Q1, it is essential that the right type of data is collected and used in automated decision-making and for the training and testing of the AI model. Therefore, there is a need to include in the data governance section a list specifying the kind of data that can be used and collected by AI-assisted decision-making tools and for the purposes of training AI models. Any social media data, for example, should not be collected and used at all as this data is not financially relevant and cannot be checked for its accuracy. In addition, to address the risk of large segments of vulnerable consumers becoming uninsurable due to the highly granular risk assessments enabled by AI, there is a need for measures that clearly stipulate how data used for risk assessments and pricing of insurance may be used to avoid excessive granularity that undermines the “risk sharing” principle of insurance. For example, the Opinion should stipulate that the use of certain proxy data like shopping behavior (e.g. using data on whether someone buys healthy foods and at what kinds of shops) to make inferences about an individual's level of risk (e.g. health risk) should be prohibited.	Noted. The Opinion is kept principle-based, with some specific and non-prescriptive examples included in the Annex. More detailed guidance may be developed in the future, where appropriate. In addition, while noting that certain variables need to be used to underwrite risks in insurance, the Opinion clarifies that undertakings should make reasonable efforts to remove biases in the data,

			including potential unlawful proxy discriminatory variables.
153	Insurance and Pensions - Denmark	Text specific comments: Point 3.18: “Data governance should ensure that the data used to train and test the AI system is complete (representative of the population and sufficient historical information), accurate (no material errors and free of bias) and appropriate (consistent with the purposes for which it is to be used). In particular, the undertaking should assess potential biases in the data and correct them in line with the undertaking’s policy.” Comment: Consider to potentially highlight that this only applies to the insurance business (Solvency II scope). Non-related / supplementing operations would not be covered. I.e. sim-ple grammar and spellchecks of texts where context is not changed or use of AI pictures for a presentation.	Noted. The Opinion has clarified that the scope of the insurance sector legislation mentioned therein is not altered, and the principles outlined in the Opinion are applicable to the use of AI systems in insurance within the scope of the Opinion, based on requirements in sectoral legislation, and following a risk based and proportionate approach.
154	Wind Tre S.p.A.	If guidelines, along with training models and AI educational policies, were centralized and made mandatory by regulation, it could ensure the highest level of protection for the end customer. Additionally, this approach would contribute to market standardization, fostering fairness and consistency in practices across the industry. Such measures would enhance consumer trust and promote ethical AI application. The data governance measures must be consistent and proportionate (taking into account the actual risk) with the measures provided for in art. 10 of the AI Act for high-risk systems. Also in this case, it is necessary to describe in more detail the commitments that weigh on providers of AI systems from those that weigh on deployers, so as to allow the appropriate fairness interventions to be carried out by the correct entity that must put them into practice.	Noted. The Opinion is kept principle-based, with some specific and non-prescriptive examples included in the Annex. More detailed guidance may be developed in the future, where appropriate.
156	ANASF	We agree that it is necessary to implement a data governance policy that complies with applicable data protection legislation, even if this entails a cost for the company to verify the standard that the data must meet. We also believe that the required standard should be certified: certification will ensure that the data used meets the standard prescribed by the legislation, especially if the company uses external data acquired from a third party.	Noted. The Opinion is kept principle-based, with some specific and non-prescriptive examples included in the Annex. More detailed guidance may be developed in the future, where appropriate.
158	BEUC - The European Consumer Organisation	-Point 3.18: BEUC recommends adding that data should be up-to-date, e.g. for consumers with a medical history, often outdated data is used (i.e. data not reflecting scientific and clinical developments of treatment) leading to outdated data (e.g. on mortality) and as a	Noted. Up-to-date data should be captured by the requirement of using

		consequence to discrimination (e.g. overpricing, exclusion, refusal of claims). When the AI system is tested, not only the impact on the general population but also on specific groups (e.g. minorities, vulnerable consumers) should be assessed to identify discriminatory practices before the AI system is rolled out to the market.	complete, accurate and appropriate data. Moreover, the Opinion includes a specific reference to vulnerable consumers in the risk-based and proportionality section, as well as in the Annex.
159	Spanish Association of Risk Management and Insurance, known as AGERS	Granularity of the data, detail, structure of the data content. Algorithms, formulas, etc. Clearly input, but output? Possibility of generating biases after analysed patterns must be analysed. That the AI does not learn that they are patterns of the entity. Validate the quality of external data sources. Obligation for a broader forum to approve the source. The objective is that it is not only the area implementing the AI that decides whether the source is reliable or not, whether it has biases or not.	Noted. The Opinion is kept principle-based, with some specific and non-prescriptive examples included in the Annex. More detailed guidance may be developed in the future, where appropriate.
160	AI & Partners	The Opinion rightly highlights the importance of robust data governance, but further emphasis on cross-border data consistency would be beneficial for insurers operating in multiple jurisdictions. A structured approach to bias detection—such as mandatory fairness audits for AI training data—would enhance consumer protection. Additionally, the Opinion should recommend best practices for handling third-party data sources, ensuring transparency in AI-driven risk assessment. Greater alignment with existing GDPR requirements and sectoral standards like the Digital Operational Resilience Act (DORA) would provide further clarity. Encouraging insurers to implement ongoing monitoring rather than one-time assessments would strengthen long-term AI governance.	Noted. The issue of cross-border data seems too detailed for this principle-based Opinion. Moreover, while noting that certain variables need to be used to underwrite risks in insurance, the Opinion clarifies that undertakings should make reasonable efforts to remove biases in the data, including potential unlawful proxy discriminatory variables. The Opinion also further elaborates on how to

			handle the challenges arising from third parties. Finally, the Opinion recognises that sound data governance should be applied throughout the AI system life cycle.
		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?	
161	BIPAR	We believe that the documentation and record-keeping requirements set out by EIOPA—particularly as detailed in the appendix—may be too granular. It is important that the level of detail required should be proportionate to the importance of the AI system to the undertaking and its impact on customers. As mentioned above, this opinion could result in unintended new requirements for intermediaries.	Noted. The Opinion acknowledges that the examples included in Annex I are not meant to be prescriptive guidance and has also highlighted that the examples included therein are mainly meant for higher risks uses of AI systems.
162	Studio legale Floreani	The section on documentation and record-keeping would benefit from more detailed provisions concerning standardisation of document formats, differentiated retention periods, and the clear allocation of responsibilities across the insurance distribution chain.	Noted. The Opinion is kept principle-based, with some specific and non-prescriptive examples included in the Annex. More detailed guidance may be developed in the future, where appropriate.
163	AFPA, Austrian Financial & Insurance Professionals Association	Dokumentation ist wichtig, muss aber zielgerichtet und verhältnismäßig sein. Standardisierte Vorlagen und Automatisierung helfen, den erforderlichen Aufwand zu reduzieren. Als Beispiel für einen proaktiven Zugang und Unterstützung durch eine Aufsichtsbehörde können nationale Datenschutzbehörden, wie jene in Österreich, genannt werden. Sobald eine für die eigene Prüftätigkeit relevante Rechtsentscheidung erfolgt, werden Auswirkungen auf die eigenen Handlungsoptionen publiziert. Weiters werden häufig gestellte	Noted. The Opinion is kept principle-based, with some specific and non-prescriptive examples included in the Annex. More detailed guidance

		Fragestellungen bzw. Problemthemen proaktiv bearbeitet und veröffentlicht. Damit können sich Unternehmen an klaren Einschätzungen bzw. Vorgaben orientiert. Dies natürlich unter Beibehaltung der Relevanz von Einzelfallentscheidungen. Die österreichische Datenschutzbehörde hat beispielsweise ein Rundschreiben zum KI-System „DeepSeek“ veröffentlicht, in welchem in einem ersten Schritt die aktive Bearbeitung kommuniziert wird und weitere Publizierung bei Neuerungen angekündigt werden. In einer ähnlich gelagerten Art und Weise wird auch in diesem Zusammenhang erwartet, dass bei gleichgelagerten bzw. aktuellen Fragestellungen die Aufsichtsbehörde proaktiv Informationen aufbereitet und einen Korridor für Lösungsmöglichkeiten vorgibt. Nur durch derartige Aktivitäten kann die Verhältnismäßigkeit gewährleistet werden. Eine weitere Möglichkeit wäre die Implementierung eines „Prüfsiegels“ durch die Aufsicht. Hier könnte beispielsweise in einem ersten Schritt durch eine „Ampel“-Bewertung (grün, gelb rot) eine transparente Bewertungsgrundlage geschaffen werden. Documentation is important but must be targeted and proportionate. Standardized templates and automation help reduce the required effort. As an example of a proactive approach and support by a supervisory authority, national data protection authorities, such as those in Austria, can be mentioned. As soon as a legal decision relevant to their own audit activities is made, the impacts on their own options for action are published. Furthermore, frequently asked questions or problem topics are proactively addressed and published. This allows companies to orient themselves to clear assessments or guidelines, while maintaining the relevance of individual case decisions. For example, the Austrian Data Protection Authority has published a circular on the AI system "DeepSeek," in which the active processing is communicated in a first step and further publications are announced for updates. In a similar manner, it is expected that for similar or current issues, the supervisory authority will proactively prepare information and provide a corridor for possible solutions. Only through such activities can proportionality be ensured. Another possibility would be the implementation of a "seal of approval" by the supervisory authority. For example, in a first step, a transparent evaluation basis could be created through a "traffic light" rating (green, yellow, red).	may be developed in the future, where appropriate.
165	Insurance Europe	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	Noted. The proportionality principle indeed applies to the Documentation and Record Keeping section of the Opinion, and the example included in the

		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.	Annex is not meant to be prescriptive and only for higher risks uses of AI systems. The Opinion clarifies that undertakings are responsible for the AI systems and data they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring.
167	Lloyd's Market Association	We agree that records of training and testing data and modelling methodologies should be kept. As paragraph 3.21 acknowledges, this duty already exists under current regulations, and documentation for AI should be handled on the same footing. Paragraph 3.23, however, is less helpful. It imports record-keeping expectations aimed at high-risk AI use cases - expectations that may not be proportionate to the use cases covered by the Opinion - and it refers to the regular review of those records. While such a review may be appropriate for high-risk systems, it is not necessarily justified in other contexts. We therefore recommend deleting paragraph 3.23.	Noted. The Opinion clarifies that the example included in the Annex is not meant to be prescriptive and only for higher risks uses of AI systems.
168	European Federation of Financial Advisers and Financial Intermediaries (FECIF)	FECIF believes that it is useful for companies to have a general list such as the one included in Annex I, indicating the documentation and records to be kept, bearing in mind that the evolutionary process of AI could lead to the need to develop and update others. This list should therefore be an ever-changing list, not definitive, to be updated periodically (for example, by checking for new developments in the market every three months).	Noted. EIOPA will indeed continue monitoring market developments and provide further guidance if appropriate.
169	AMICE	While we acknowledge the importance of maintaining records for AI processes, we find EIOPA's documentation requirements, especially those in the appendix, too detailed and prescriptive. The level of detail should match the AI system's significance and its impact on customers.	Noted. The Opinion clarifies that the example included in the Annex is not meant to be prescriptive

			and only for higher risks uses of AI systems
170	Institute of International Finance	We would firstly suggest, as mentioned above, that the material put forward in Annex I relating to “high-risk AI use cases” may not belong in the Opinion, for the reasons set out in relation to para 2.6 above. If it is retained, the distinction drawn between a high-risk AI system and high-risk use case need to be better explained by reference to the concepts in the AI Act. Secondly, while we welcome that it is recognised that record-keeping with regard to AI systems should be done ‘taking into account risk-based and proportionality considerations’ (para 3.22), we are concerned that the documentation examples set out in Annex I to the Opinion are extensive and could become de facto requirements despite the Opinion’s stated intent. Competent authorities may take these as a template for a tick-box compliance exercise without regard for proportionality or indeed risk. Any documentation provisions should be advisory only and should be principles-based rather than prescriptive, focusing on material risk controls and considerations. Again in this section EIOPA does not consider the case when an insurance company acquires the AI system by a third party. In this situation the compliance with the record keeping requirements, as defined in the appendix, would be impracticable. Indeed, when qualifying merely as a deployer, the insurance company may not have access to all the information that EIOPA is suggesting to keep, such as information on data collection and preparation, the dataset itself used for training the AI system, and the code on which the AI system is based. To solve this problem, EIOPA should clearly distinguish the roles of AI developers and deployers and the respective record-keeping expectations in its guidance.	Noted. The Opinion explains that the proportionality principle is applicable to all the governance and risk management measures described in the Opinion. The Opinion also clarifies that the example included in the Annex is not meant to be prescriptive and only for higher risks uses of AI systems. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems and data they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring.
171	Gesamtverband der Deutschen Versicherungswirtschaft	EIOPA proposes that insurance companies should have adequate records of training and test data and modelling methods. The requirements are obviously based on the requirements of the AI Act for high-risk AI systems. It should therefore be made clear that no extension to non-high-risk systems is intended. Insurance companies that have purchased AI systems from third-party providers may not	Noted. The Opinion clarifies that it does not set out new requirements and does not seek to alter the scope of the AI Act by extending the requirements of the AI Act for high-risk AI

		have all the data that EIOPA proposes in the opinion (e.g. the data sets used for training, the code on which the system is based), so it would be important to distinguish between the roles of deplpoyers and providers and to consider separate record-keeping expectations. If insurance undertakings use AI systems that they have obtained from third parties, it should be sufficient to take reasonable steps to obtain relevant information from the AI system provider, who is legally obliged to share transparency-related documentation about their products.	systems to all AI systems used in insurance. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems and data they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring.
172	CNP Assurances	The approach here is also too general and generic. CNP Assurances is asking for more precision on the expectations in terms of reproducibility, the level of documentation required and the management of evolving AI systems. A proportionate approach, for the long-term follow-up file tracking, and a greater focus on post-deployment monitoring, would help to ensure practicality and environmental sustainability. Regarding point 3.22, a basic set of information is required to keep an adequate follow-up of AI systems. This information must be specified and must be subject to checks. CNP Assurances suggests providing more specific guidance on post-deployment monitoring. If annex I contains useful examples, the link between these and the supervisory obligations set out in the main text could be strengthened. Additionally, model limitations, built-in assumptions, and intelligibility should be discussed more clearly, preferably in a separate documentation section. Incorporating guidance on the geographic location of data storage is significant for data protection, operational resilience, and cybersecurity. Understanding data sovereignty and regulatory requirements related to storage location is increasingly crucial for insurers conducting business internationally.	Noted. As previously explained, the Opinion is kept principle-based, with some specific and non-prescriptive examples included in the Annex. More detailed guidance may be developed in the future, where appropriate. The Opinion clarifies that the example included in the Annex are meant to illustrate possible ways of implement the provision of the Opinion in practical ways, but at the same time it is not meant to be prescriptive and only for higher risks uses of AI systems.

		Section 1 of Annex I includes headings like 'severity' and 'likelihood,' which may lead companies to quantify risks that should be addressed qualitatively. Removing these labels or clarifying their purpose could prevent misinterpretation. Finally, we suggest removing references to high-risk AI use cases in the sample documentation, as these are outside the scope of the opinion. The inclusion of such examples may confuse the applicable expectations. The documentation required for high-risk AI systems (Appendix I) should be adaptable for other AI systems, in order to make the opinion more relevant: we have identified a need for documentation for (1) the data that should make it possible to verify the proper record keeping of the information from the point of view of governance and elements in relation to their processing; (2) algorithms, so as to have a set of information that makes transparent the theoretical choices made and the type of choices made on key parameters; (3) the generation of outputs and tests, aimed at having clear information on the results and their robustness, both for validation and use purposes; (4) on the system that hosts the AI systems, so as to produce a clear understanding of the pipeline and the safety rules implemented.	The issue of the location of data storage seems too detailed for the purpose of the Opinion, but further guidance on this and other topics mentioned in the comments may be provided at a later stage, where relevant, also in view of the requirements under DORA.
173	IRSG	In this section, the Opinion is not very precise, because it establishes documentation and record keeping requirements without distinguishing between the case in which the insurer is the developer or only the deployer. In the latter case, which is very common, it is clear that the insurer will not simply have access to technical data that is in the hands of the developer: information on data collection and preparation, the dataset itself used for training the system and the code on which the AI system is based. Moreover, this information, like the code itself, may be protected by trade secrets of the company that created it. Clarification is therefore needed. The example given in Annex I referred to in sect. 3.23 is not very useful, as it is intended for high-risk AI systems. An example should be proposed that applies to non-high risk systems, which are the subject of this Opinion, and distinguishing between cases where the insurer is a developer and the insurer is only a deployer. At the same time, it should be borne in mind that the fact that the insurer outsources this service does not in any way relieve it of liability, as is the case under Article 49 of the Solvency II Directive. Therefore, the solution proposed by EIOPA should be very carefully considered, as it should provide for realistic measures in the event that the insurer is only a deployer and, at the same time, without the outsourcing of the service being a way of releasing the insurer from liability against the provisions of Art. 49 Solvency II. On the other hand, the Opinion is so brief on this point that it also fails to address another relevant question, which has been the subject of debate within the IRSG and on which there	Noted. The Opinion explains that the proportionality principle is applicable to all the governance and risk management measures described in the Opinion, including the documentation and record keeping section. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems and data they use, even if provided by third parties, and should take steps to ensure proper governance and risk

		are opposing positions: should the same level of documentation and record keeping be required for all (not high-risk) AI systems used by an insurance undertaking, or, on the contrary, should a distinction be made between those that might not have a significant impact on the company, employees or on consumers and those where there might be such impact? Some members in the IRSG are of the opinion that, because of the principle of proportionality, if an AI system does not have a clear impact on the company or consumers, but only has internal effects (e.g. the system for regulating the temperature in the office), it should not be subject to the same regime as those where there might be an appreciable impact. Against this position, it is contested that such a distinction is inappropriate, arguing that every AI system has different levels of environmental and social impact, direct or indirect. Established social dialogue and consultation procedures for discussions about the extent to which AI systems have a significant impact on business, consumers or employees are significant here. By this the insurers also cover principal features, emphasizing the importance of transparency and human oversight in deployment in general. Ultimately, it would be advisable for the Opinion to reflect whether the same measures should apply to all not high-risk AI systems, or whether a distinction should be made on the basis set out above.	management as relevant, including for instance through contract clauses, audits, and monitoring. The Opinion clarifies that the example included in the Annex is not meant to be prescriptive and only for higher risks uses of AI systems.
174	CRO Forum	We support the clear reference to the need for a proportionate and risk-based approach in documentation and record keeping on AI Systems. In paragraph 3.22, EIOPA suggests that undertakings should keep appropriate records of the training and testing data and the modeling 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/information. Information on retraining data sets should also be considered in line with a proportional and risk-based approach. For example, AI deployers don‘t always have access to all information that EIOPA is suggesting (eg dataset used for training, the code on which the system is based). We recommend distinguishing between the roles of AI deployers and providers and consider separate record-keeping expectations. Paragraph 3.23 refers to ‘high risk’ models, which the Opinion has previously stated are excluded from its scope, so, this section could be confusing.	Noted. The Opinion explains that the proportionality principle is applicable to all the governance and risk management measures described in the Opinion, including the documentation and record keeping section. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems and data they use, even if provided by third parties, and should take steps to ensure proper governance and risk

			management as relevant, including for instance through contract clauses, audits, and monitoring.
175	European Financial Congress	EIOPA's opinion indicates that even for less risky AI applications in insurance, adequate documentation is expected to be maintained, although the scope and detail are to be tailored to the level of risk. In this sense, EIOPA's requirement goes beyond the literal wording of the AI Act, which does not impose such detailed documentation obligations on not-high-risk systems. For low- to medium-risk AI systems, for which the AI Act does not impose such detailed documentation requirements, the need to maintain records of training data, testing data and modeling methodologies may generate additional costs and workload. Insurers will need to implement additional processes, IT tools and compliance procedures, even for less significant AI applications. The provision refers to "appropriate records," which leaves wide room for interpretation as to how detailed documentation should be in practice for less risky applications. This could lead to regulatory uncertainty and divergent approaches by national supervisors. If the requirement is interpreted strictly, it could discourage the implementation of innovative, low-risk AI solutions in the insurance industry, due to disproportionate costs	Noted. The Opinion explains that the proportionality principle is applicable to all the governance and risk management measures described in the Opinion, including the documentation and record keeping section. Concerning the reference to divergent approaches, the Opinion is kept principle-based, with some specific and non-prescriptive examples included in the Annex. More detailed guidance may be developed in the future, where appropriate.
176	European Confederation of Institutes of Internal Auditing	-We encourage EIOPA to make a clear distinction between internal and external audit. In the current text, EIOPA is speaking about “audit”. -We remind that Internal Auditors follow international standards (Global Internal Audit Standards set up by IIA Global that requires internal audit functions to have a Quality Assurance and Improvement Program (QAIP) in place. The quality assurance review evaluates the efficiency and effectiveness of the internal audit function. The review must take place every 5 years, by an external provider and it is part of the monitoring of the governance process by management and the audit committee. The internal audit function reports directly to the board, enabling it to perform its duties in an independent manner. The internal audit function plays a key role in the assessment of the product approval process. It includes the controls in place, the governance and not just the	Noted. The reference to the difference between internal and external audits is considered to be too detailed for the present Opinion, which is kept principle-based, with some specific and non-prescriptive examples included in the Annex. More detailed guidance may be developed in the future, where appropriate.

		documentation.	The focus is in general on internal audit and aims to be flexible in view of the split of functions and responsibilities in an undertaking, so long as there is appropriate senior management accountability overall.
177	BETTER FINANCE	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.	Noted. The Opinion is in line with this comment; by stating that, following a risk-based and proportionate approach, undertakings should keep appropriate records of the training and testing data and the modelling methodologies to enable their reproducibility and traceability.

178	Actuarial Association of Europe	Key message: The AAE agrees with the importance of robust documentation and record-keeping for AI systems. However, we suggest EIOPA clarify expectations around reproducibility, the level of documentation required, and how evolving AI systems should be treated. A proportionate approach, particularly for long-term record tracking, and greater attention to post-deployment monitoring, would help ensure practicality and environmental sustainability. Detailed response: We support EIOPA's emphasis on appropriate documentation and record-keeping to support accountability and transparency. These are critical for effective governance and should be aligned with existing risk management practices. A key point requiring clarification is the expectation of reproducibility and traceability. In practice, many AI systems—especially those involving automated machine learning or stochastic elements—may not allow for strict reproducibility. Some models also operate as black boxes. We encourage EIOPA to clarify whether reproducibility is an "obligation of results" (i.e., a hard requirement), or an "obligation of means" (i.e., reasonable effort to achieve it). A balance should be struck between ideal expectations and technical realities. Also, we suggest that the level of technical detail required in documentation should be proportionate to the context and consistent with expectations for non-AI models already subject to governance under existing risk management systems. Overly detailed technical documentation may not always be practical or necessary. The Opinion could also provide more structured guidance on post-deployment monitoring. While Annex I contains useful examples, the link between these and the monitoring obligations in the main text could be strengthened. Moreover, aspects such as model limitations, embedded assumptions, and interpretability merit more explicit treatment, ideally as a distinct documentation topic. Regarding long-term data record tracking, we propose a proportionate approach based on the function and sensitivity of the AI system. Continuous storage of large datasets can carry a high environmental cost, and requirements should be calibrated accordingly. We also suggest including guidance on the geographic location of data storage, given its relevance for data protection, operational resilience, and cybersecurity. Awareness of data	Noted. Following a risk-based and proportionate approach, when there are challenges to ensure traceability and reproducibility undertakings may put in place complementary governance and risk management measures, where relevant. The issue of the location of data storage seems too detailed for the purpose of the Opinion, but further guidance on this and other topics mentioned in the comment may be provided at a later stage, where relevant. The Opinion clarifies that the example included in the Annex is not meant to be prescriptive and only for higher risks uses of AI systems.

		sovereignty and regulatory obligations tied to storage location is increasingly important for insurers operating cross-border. From a usability perspective, we note that some elements in Annex I Section 1—such as "severity" and "likelihood" headings—may prompt undertakings to quantify risk factors that are better addressed qualitatively. Removing these labels or clarifying their purpose could prevent misinterpretation. Finally, we recommend removing references to high-risk AI use cases in the documentation examples, as these fall outside the scope of the Opinion. Including such examples may cause confusion for undertakings trying to understand the applicable expectations.	
179	Insurance and Pensions - Denmark	Text specific comments: Point 3.22: "In the context of AI systems, and taking into account risk-based and proportionality considerations, undertakings should keep ap-propriate records of the training and testing data and the modelling methodologies to ensure their reproducibility and traceability." Comment: Consider to potentially highlight that this only applies to the insurance business (Solvency II scope). Non-related / supplementing operations would not be covered. I.e. sim-ple grammar and spellchecks of texts where context is not changed or use of AI pictures for a presentation. Point 3.23: "An example of the types of records and documentation that should be kept and reviewed on regular basis for higher risk AI use cases is provided in Annex I." Comment: As Annex I is clearly introduced as an example another wording than "should" would be preferred to clarify this. Specific comments on Annex I: As there is no question in the consultation directly aimed at the Annex-es, we will address Annex 1 here. Comments on "2. EXAMPLE OF RECORD KEEPING FOR HIGH-RISK AI USE CASES"	Noted. The Opinion provides guidance on how to interpret various provisions of the existing insurance sectoral legislation in the context of AI systems. The scope of the insurance sector legislation mentioned therein is not altered, and the principles outlined in the Opinion are applicable to the use of AI systems in insurance within the scope of the Opinion, based on requirements in sectoral legislation, and following a risk based and proportionate approach. The Opinion clarifies that the example included in the Annex is not meant to be prescriptive and only for higher risks uses of AI systems.

		@Technical choices / arbitration: The inclusion of “Ethical” in the last sentence cannot be inferred from the current regulation. Consider de-leting “Ethical” in the sentence and instead ad a new sentence i.e.: “Where relevant ethical considerations can also be recorded.” after the current sentence. @Model performance: The inclusion of “Ethical” in the last sentence cannot be inferred from the current regulation. Consider deleting “Ethical” in the sentence and add “Where relevant ethical considerations can also be recorded.” after the current sentence. @Model security: In the first sentence we would suggest to add “ade-quately” as complete protection is not possible. This would also be in line with proportionality considerations. I.e. “To ensure that the model is adequately protected from outside at-tacks…” @Ethics and trustworthy assessment: We would suggest that this sec-tion should be removed or listed as “additional consideration” as a gen-eral requirement for ethics and trustworthiness assessments does not follow from current regulation. Comments on “3. EXAMPLES OF FAIRNESS METRICS”: @Equalized Odds, Equalized Opportunities and Individual fairness: These last 3 sections “Equalized Odds”, “Equalized Opportunities” and “Individual fairness” should be listed as additional considerations as they cannot be inferred as general requirements from current regula-tion. In the section Equalized Odds it could be considered to use another example as recruitment is not in scope of insurance regulation.	Moreover, the references in the Annex have not been amended given that they reflect the work of EIOPA’s Consultative Expert Group on Digital Ethics in insurance. However, as previously mentioned, it has been clarified that they are included as illustrative examples and should not be considered as prescriptive guidance.
180	Wind Tre S.p.A.	As per previous comment,If guidelines, along with training models and AI educational policies, were centralized and made mandatory by regulation, it could ensure the highest level of protection for the end customer. Additionally, this approach would contribute to market standardization, fostering fairness and consistency in practices across the industry. Such measures would enhance consumer trust and promote ethical AI application. The measures on documentation and record keeping must be consistent and proportionate	Noted. As previously explained, the Opinion is kept principle-based, with some specific and non-prescriptive examples included in the Annex.

		(taking into account the actual risk) with the measures provided for in art. 11 and 12 of the AI Act for high-risk systems. Also in this case, it is necessary to describe in more detail the commitments that weigh on providers of AI systems from those that weigh on deployers, so as to allow the appropriate fairness interventions to be carried out by the correct entity that must put them into practice.	More detailed guidance may be developed in the future, where appropriate.
182	ANASF	We believe that it is useful for companies to have a general list such as the one included in Annex I, indicating the documentation and records to be kept, bearing in mind that the evolutionary process of AI could lead to the need to develop and update others. This list should therefore be an ever-changing list, not definitive, to be updated periodically (for example, by checking for new developments in the market every three months).	Noted. The Opinion clarifies that the example included in the Annex is not meant to be prescriptive and only for higher risks uses of AI systems. EIOPA will indeed continue monitoring market developments and provide further guidance if appropriate.
183	BEUC - The European Consumer Organisation	- Point 3.22: “Appropriate” records can interpreted in a divergent manner, we encounter currently the situation that AI systems are held as a black-box with no information provided on which data is used and the modelling methodologies. We consider that full access to such data is key for supervisors is key to allow for appropriate supervision of AI systems. The decision of how much data needs to be recorded and documented should not be left to the insurance operators. - Point 3.23: Annex I is labelled as the requirements for records and documentation for “high risk” AI which is applies pursuant to the AI Act only to a very limited set of insurances. BEUC recommends establishing instead a specific list of requirements of the high-risk AI systems to ensure that it is sufficiently precise for the assessment. In addition, it should not be established just as an example but as mandatory requirements. As regards training data, it should be clarified that it is not sufficient to record the variables with their respective domain range but the actual data including their origin allowing to assess the data quality for the specific use case. For the other types of AI systems, not classified as high-risk, an additional annex of minimum requirements for the recording and documentation should be set up. Otherwise, the opinion gives the impression that insurance operators can freely decide how to document and record for AI systems not qualified as high-risk.	Noted. The Opinion explains that, following a risk-based and proportionate approach, undertakings should keep appropriate records of the training and testing data and the modelling methodologies to enable their reproducibility and traceability. The Opinion clarifies that the example included in the Annex is not meant to be prescriptive and only for higher risks uses of AI systems. EIOPA will continue monitoring market developments and provide

			further guidance, where appropriate.
184	Spanish Association of Risk Management and Insurance, known as AGERS	Documentation and record-keeping are essential to ensure the traceability and reproducibility of the AI systems used by insurers. According to the document 'Impact Assessment of EIOPA's Opinion on AI governance and risk management', several key points stand out: • Relevance of documentation: Article 258(1)(i) of Delegated Regulation 2015/35 requires insurers to keep adequate and orderly records of their business and internal organisation. This is crucial for traceability and accountability in the use of AI systems (p. 9). • Proportionality: Documentation should be adequate and proportionate to the risks and characteristics of the use of AI. This involves keeping detailed records of training and test data, as well as the modelling methodologies used (p. 6). • Examples of records: The document provides specific examples of the types of records that should be kept, such as the explanation of the business objective, integration into the IT infrastructure, data collection and preparation, technical choices and model security (p. 15). Other measures to consider: • Regular audits: Implement regular audits to review and update records and documentation, ensuring that they reflect changes and improvements in AI systems. • Quality standards: Define and apply quality standards for documentation, ensuring that all records are complete, accurate and accessible. • In addition to these measures, we can highlight and consider it important to address:- The implementation of record management tools: Use advanced record management tools that facilitate the organisatio n, search and retrieval of documentation related to AI systems. - Training: Provide ongoing training to employees on the importance of documentation and best practices for maintaining proper records. Record keeping: According to Regulation (EU) 2024/1689, high-risk AI systems must allow for the automatic recording of events throughout their lifetime. This is essential for the traceability and transparency of the system's operation, and will enable it to respond to requests from consumers and users exercising their rights of access and information.	Noted. The Opinion is kept principle-based, with some specific and non-prescriptive examples included in the Annex. More detailed guidance may be developed in the future, where appropriate.

		In short, we consider it essential to define specific rules that address the elements and define standards on record keeping, support the training of key members of corporations, and encourage the implementation of risk management tools that can measure in real time the development of AI systems within the framework of insurance entities.	
185	Chika Okoli	1) AI exposure addendum to the CTP register for EU DORA compliance: As mentioned in Q4, identifying the material use of AI among AI among CTPs would help document the AI risk exposure. 2) Document Critical Processes impacted/aided by AI Beyond documenting Ai exposure among CTPs, mapping and documenting the AI use for critical processes would be key to uncovering latent AI risks that might not be captured among CTP registers (with AI risk addendums).	Noted. In line with its principle-based approach and taking into account the on-going work in DORA concerning critical third parties, the Opinion does explicitly mention the latter, but EIOPA will continue monitoring market and legislative developments and provide further guidance, were appropriate.
186	AI & Partners	Strong documentation is essential for AI accountability, and the Opinion correctly emphasizes this. However, it should provide more detailed guidance on the granularity of records insurers must maintain, particularly for higher-risk AI applications. Developing standardized AI model documentation templates could improve consistency across the industry. Additionally, requiring version control and tracking of AI system changes—similar to regulatory expectations for financial models—would enhance transparency. Insurers should also document model performance monitoring, including error rates and mitigation actions taken over time. Aligning AI documentation requirements with broader IT governance standards would streamline compliance efforts.	Noted. The Opinion is kept principle-based, with some specific and non-prescriptive examples included in the Annex. More detailed guidance may be developed in the future, where appropriate.
		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?	
187	BIPAR	Intermediaries (and consumers) should be informed if pricing, claims or selection (anti-selection) decisions are made on the basis of AI. This would ensure that the AI based decision can be challenged in the interest of the consumer. As mentioned in our response to question 3, it is important that distributors are informed through adequate information flows on the models adopted and the use of AI systems by manufacturers to ensure they can inform their customers accordingly (see point 3.27).	Noted. The Opinion also includes a reference of the need of insurance intermediaries to obtain sufficient information from insurance undertakings in order to meet their

		It may not fully address some practical trade-offs between AI accuracy, efficiency, and compliance with insurance-specific regulations. We therefore suggest that a hybrid AI model approach, where unexplainable AI models (such as LLM, neural networks, deep learning, advanced ML etc) are combined in the final stage of certain sensitive processes with explainable models. Some examples of such processes where a hybrid AI approach could be used: - interaction assisting in the evaluation of an insurance contract or in the decision of accepting or rejecting a claim, - an underwriting or pricing decision or other processes affecting consumers rights or solvency of the undertaking. Such a hybrid approach where the final layer of the decision becomes explainable will allow for reducing the asymmetry between the undertaking and the consumer. It would also allow intermediaries to inform consumers as they will have access to relevant information. This hybrid approach would effectively balance AI performance and efficiency, regulatory compliance and consumer protection together with human oversight and auditability.	obligations towards customers. The Opinion also acknowledges the trade-off between accuracy and explainability and emphasises the need to follow a risk-based and proportionate approach.
188	Studio legale Floreani	To ensure genuine transparency in the use of AI in insurance distribution, disclosures should be adapted to client profiles, supported by multi-layered explanations (technical and non-technical), and subject to minimum clarity requirements. It is recommended to: Develop templates specifically designed for insurance intermediaries Provide clear and shared terminological glossaries Implement client feedback mechanisms and comprehension testing Align requirements with IDD, GDPR and consumer protection frameworks	Noted. The Opinion clarifies that the explanations should be adapted to the needs of different recipient stakeholders. The Opinion is kept principle-based, with some specific and non-prescriptive examples included in the Annex. More detailed guidance may be developed in the future, where appropriate.
189	AFPA, Austrian Financial & Insurance	Wie bereits unter Frage 3 ausgeführt, ist hier eine hohe Abhängigkeit in Bezug auf die KI-Anbieter gegeben.	Noted. The Opinion clarifies that undertakings are responsible for the AI

	Professionals Association	Kunden müssen bei Einsatz von KI umfassend und verständlich informiert werden. Dies ist unmöglich, wenn die KI-Anbieter nicht umfassend kooperieren und die erforderlichen Informationen zur Verfügung stellen As already stated under question 3, there is a high dependency on AI providers. Customers must be comprehensively and understandably informed when using AI. This is impossible if the AI providers do not fully cooperate and provide the necessary information.	systems and data they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring.
190	Insurance Europe	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	Noted. The Opinion has clarified that the scope of the insurance sector legislation mentioned therein is not altered, and the principles outlined in the Opinion are applicable to the use of AI systems in insurance within the scope of the Opinion, based on requirements in sectoral legislation, and following a risk based and proportionate approach. The Opinion explains that undertakings should adapt the explanations to specific uses of AI systems and to the different recipient stakeholders of the explanations. The Opinion also recognises that if the complexity of the AI system hinders the full transparency and explainability, the

		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.	undertaking should put in place, where necessary, complementary risk management measures such as stronger guardrails and increased human oversight. Undertakings should comprehensively secure and test - before release as well as on an ongoing basis - those uses of AI systems that could have a high impact on customers or the solvency of the undertaking.
192	Lloyd's Market Association	We generally agree with this section. Whilst we fully support the expectation that AI systems, especially those affecting customer outcomes, must be explainable and auditable, this should be tempered with practical recognition of technological constraints. Some AI models (e.g. deep neural networks) inherently lack transparency. Where third-party vendors provide AI capabilities, insurers may face limits in their ability to provide full explanations. We therefore believe that expectations on due diligence and oversight of third-party AI providers be calibrated to avoid disproportionate burden, particularly where market-wide vendor reliance exists and contractual influence is limited. We would point out that this quandary is nothing new and is similar to the questions over the use of tech providers in material outsourcing where the undertaking has limited power over contracts. This may require more consideration from the regulators. We would point out that paragraph 3.25 could be construed as limiting the use of "complex AI systems" to challenging and fine tuning traditional mathematical models. Whilst we believe this is not the intention and is merely an example of an approach that could be taken, we think that the current framing will be construed by some as a requirement, limiting such undertaking's ability to exploit the full future potential of AI. EIOPA should be mindful of the risk of such examples being construed as such.	Noted. The Opinion recognises that if the complexity of the AI system hinders full transparency and explainability, the undertaking should put in place, where necessary, complementary risk management measures such as stronger guardrails and increased human oversight. Undertakings should comprehensively secure and test - before release as well as on an ongoing basis - those uses of AI systems that could have a high impact on customers or the solvency of the undertaking.

			Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems and data they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring. Finally, the examples mentioned in former paragraph 3.25 are not exhaustive.
193	Dr. Paul Larsen	In my opinion, it is essential to keep the current wording in * 3.25 about recognizing and documenting the limitations of XAI current techniques and tools * 3.26 about complementary risk management measures (though there is a minor typographical error: "complementay" instead of "complementary") * 3.27 about adapting the explanations to relevant stakeholders as the current wording reflects the currently less-than-satisfactory state of the field of explainable AI.	Noted. The wording has been kept as suggested. The typo has also been corrected.
194	European Federation of Financial Advisers and Financial Intermediaries (FECIF)	We agree, it seems clear and effective to us.	Noted.
195	AMICE	As already pointed out in our answer to Q6, the Opinion seems to extend the transparency requirements provided under the Commission Delegated Regulation 2015/35 beyond their original scope and without an adequate legislative basis. We therefore suggest narrowing the scope of the relevant expectations.	Noted. The Opinion has clarified that the scope of the insurance sector legislation mentioned therein is not altered, and the principles outlined in the Opinion are applicable

			to the use of AI systems in insurance within the scope of the Opinion, based on requirements in sectoral legislation, and following a risk based and proportionate approach.
196	Institute of International Finance	As a general comment, EIOPA should limit the transparency and explainability discussion to the areas of underwriting, reserving, and technical provisions, which are explicitly referred to in those legislative acts that are cited in para. 3.24 as the legal basis. It should not go beyond and try to "fill in the gaps" in its mandate. We welcome the recognition that 'Different approaches can be used' (para 3.25) regarding explainability methods, which allows for flexibility in implementation. We appreciate the recognition of 'explainable AI algorithms instead of more opaque ('black box') ones' (para 3.25) as one potential approach, acknowledging the spectrum of explainability in different AI techniques. The Opinion notes specific explainability tools (LIME/SHAP) (para 3.25). While this shows awareness of current industry practice, we consider it undesirable to endorse or 'call out' particular industry solutions given the speed of development in this space.	Noted. The Opinion has clarified that the scope of the insurance sector legislation mentioned therein is not altered, and the principles outlined in the Opinion are applicable to the use of AI systems in insurance within the scope of the Opinion, based on requirements in sectoral legislation, and following a risk based and proportionate approach. Moreover, the references to LIME and SHAP have been moved to a footnote to keep the text of the Opinion adaptable to potential future developments in this area.
197	Gesamtverband der Deutschen Versicherungswirtschaft	The section on transparency and explainability seems to be based on Art. 13 of the AI Act on 'Transparency and provision of information to operators', which refers exclusively to high-risk AI applications. Therefore, the EIOPA opinion should clarify that it does not extend these requirements to non-high-risk AI systems. It is also problematic that the requirement in 3.27 to provide an explanation in 'simple, clear and non-technical language' even goes beyond the requirements of the AI Act. This point should therefore be deleted.	Noted. The Opinion has clarified that it does not set out new requirements and does not seek to alter the scope of the AI Act by extending the requirements of the AI Act for high-risk AI systems to all AI systems.

			Moreover, the principles outlined in the Opinion are applicable to the use of AI systems in insurance within the scope of the Opinion, based on requirements in sectoral legislation, and following a risk based and proportionate approach.
198	CNP Assurances	Transparency and explainability are key elements in facilitating greater public understanding and trust in the use and application of AI. It is fundamental to adopt a proportionate and contextual approach to explainability, and to clarify whether it is an obligation of means or of results. The opinion should be neutral and avoid focusing on specific methods. Explainability is not always appropriate in all cases. In practice, many models cannot be fully explained, especially complex or black-box systems. Thus, "black box" AI models limit the trust and monitoring (improvement) of algorithms. In the presence of AIS that is too complex for a human to understand, an additional method or technique to be able to access the black box and understand how the model works may be required. The opinion currently refers to specific technical tools – LIME and SHAP – as examples of explainability techniques. While illustrative, naming these methods may inadvertently give the impression that peculiar tools are approved. Revise the wording by referring instead to "local and global methods independent of the model", with supporting examples. This approach avoids prescribing specific methodologies and allows companies to choose the appropriate tools based on their use case. Transparency and explainability monitoring systems require: 1. A more detailed overview of the entry and exit process; 2. A clear documentation of the techniques used to support explainability (model-specific or not); 3. An access to the results of agnostic or model-specific techniques, used in the form of a user guide and dashboard, including elements such as: (i) the importance of characteristics overall or by individual prediction (in the form of summary graphs) (ii) dependency diagrams to confirm or dispute the results of summary diagrams or other aggregate measures of characteristic importance.	Noted. The references to LIME and SHAP have been moved to a footnote to keep the text of the Opinion adaptable to potential future developments in this area, and the proposed wording has been incorporated into the text. Concerning the other suggestions about transparency and explainability monitoring systems, the Opinion is kept principle-based, with some specific and non-prescriptive examples included in the Annex. More detailed guidance may be developed in the future, where appropriate.

199	IRSG	The broad scope of application of EIOPA's transparency and explainability requirements, which appear to cover all AI systems used by an insurance company, raises concerns. One of them is the very meaning of the term "explainability" (or "meaningfully explainable"), which is used by EIOPA in sect. 3.25, because for AI practitioners it has not one but several meanings. It could mean: (i) ensuring that particular outputs of AI models are explainable; (ii) ensuring that the processes by which a model reaches a decision are explainable; (iii) ensuring that firms need to explain their approach to AI governance. Given the state of AI technology and current levels of understanding as to how AI models function, it may not be technically possible for firms to achieve the first two definitions of "explainability" above, although the achievability of the regulator's ambition will depend in large part on how EIOPA defines "explainability". We do not think that the adjective "meaningful" adds much in 3.25 above: it is not clear what difference it makes for something to be "meaningfully explainable" or "explainable" when the meaning of "explainable" is fundamentally ambiguous. Therefore, we recommend that EIOPA avoids issuing new guidance in this area straightaway but instead convenes discussions with industry firms to understand how firms are explaining AI decisions, how far firms find that it is technically possible to explain AI usage, what tools firms are using to explain AI, and what kind of guidance EIOPA could issue to help firms know what they need to do in this area to provide customers and clients with helpful explanations about AI decisions. However, if EIOPA decides to issue guidance without this previous discussion, we would encourage it to qualify 3.25 above and offer more proportionate explainability guidance. For example, EIOPA could more explicitly acknowledge complexities around AI explainability (including the ambiguous meaning of "explainability"). EIOPA could say that firms should strive for explainability (and document how they are doing this) but recognise that fully satisfying explainability may not always technically be possible. On the other hand, if EIOPA intends to proceed with issuing guidance on this matter, we recommend EIOPA adopt a proportionate approach, ensuring that less burdensome requirements apply to AI systems that do not impact customers. In this regard, it is important to highlight that Delegated Regulation n. 2015/35, referenced by the Opinion as legal basis, imposes transparency requirements for a well-defined set of information systems, namely those related to the company's business, activities,	Noted. The Opinion is kept principle-based, and its content and terminology used is consistent with similar references in sectoral legislation as well as in other regulations such as the GDPR or the AI Act. Furthermore, more detailed guidance may be developed in the future, where appropriate. The Opinion also acknowledges the trade-off between accuracy and explainability and emphasises the need to follow a risk-based and proportionate approach. The references to LIME and SHAP have been moved to a footnote to keep the text of the Opinion adaptable to potential future developments in this area. EIOPA will indeed continue monitoring market developments via different tools in close collaboration with stakeholders, and it envisages to subsequently develop more detailed analysis on specific AI

		commitments and risks. We therefore encourage EIOPA to align its transparency expectations with the existing legislative framework and further integrate the principle of proportionality into its recommendations. The transparency required would include aspects as varied as the need to provide answers to clients asking about the extent to which biases have been addressed and removed. Additionally, to ensure that the guidelines remain technologically neutral and adaptable to future technological advancements, we recommend that EIOPA remove specific references to LIME and SHAP in sect. 3.25. While these tools are currently widely used, referencing specific methodologies may limit flexibility and could quickly become outdated. Rather than appearing to recommend specific tools, EIOPA might instead direct firms towards guidance produced by other public bodies on how to explain decision made with AI. One example is the UK Information Commissioner's Office (ICO) guidance on Explaining decisions made with AI. In this sense, we would urge it to institute regular reviews of such guidance to ensure it is keeping pace with technological developments. It is easy to imagine a situation in which further AI developments render various of kinds of explainability easier or harder to achieve. A more principle-based approach would better support long-term applicability and innovation in AI governance. In light of the above, if EIOPA finally decides to issue guidance on this matter, we suggest amending sect. 3.25 as follows: "Undertakings should adopt the necessary measures to ensure that the outcomes of relevant AI systems, particularly those affecting business activities, commitments, and risks, can be meaningfully explained. Different approaches can be used to this extent, such as using explainable AI algorithms instead of more opaque ("black box") ones, or using complex AI systems only for the purpose of challenging and fine-tuning traditional mathematical models. A variety of supplementary explainability tools such as LIME or SHAP may also be used to explain the inner functioning of complex AI systems, but provided that the limitations of these tools should be duly documented and addressed".	systems or issues arising from the use of AI systems in insurance and provide further guidance, where appropriate.
200	CRO Forum	We welcome EIOPA's emphasis on explainability of AI. We consider that explainability and transparency are a precondition for the understanding of and trust of AI. However, we would like to stress that explainability may not be suitable in every situation. Depending on the context, requiring explainability could affect the accuracy and performance of the AI system or introduce privacy and security risks. To this end, insurance companies should, for example, not be required to explain AI that they use for fraud detection or to prevent the risk	Noted. The Opinion clarified that undertakings should adapt the explanations to specific uses of AI systems and to the needs of different

		of model manipulation or exploitation. Insurers may also be deployers of AI and EIOPA stresses that the AI system should perform consistently throughout their lifecycle, regardless of whether they have been developed in-house or purchased from third-party service providers. We would recommend that EIOPA clarify the responsibility of providers of AI, where insurers leverage the AI provided by such third-party providers, consistent with the EU AI Act. In paragraph 3.25, explainability can be defined as the ability to articulate and understand how the AI systems operate and increases the overall understanding and ability to manage the risks of the AI system. The degree of transparency and explainability should be proportionate to the risk(s) presented by the AI system and take into account their adaptive and autonomous nature. Paragraph 3.25 implies that firms should avoid using more complex AI models, other than to test or fine tuning more traditional models. This could overly constrain insurers' ability to leverage the opportunities from more complex models that may not impact customers or financial models. Paragraph 3.26 lists risk management techniques for more complex AI models and therefore contradicts 3.25, which implies more complex AI models should not be used (except for challenging or fine tuning of more traditional models). Many of the explainability and transparency issues associated with AI are not new, and in many cases risk management measures are already in place including privacy notices. Firms could also ensure their complaints / appeal process can facilitate challenge and deliver redress for any AI System outcomes, if required. On a proportional basis, for more high-risk AI Systems, firms could consider a transparency assessment.	recipient stakeholders; while full explanations towards customers may not be appropriate in certain circumstances and uses of AI systems, undertakings should be able to provide appropriate explanations to other stakeholders such as supervisors. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems and data they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring. The Opinion explains that the risk-based approach and the proportionality principle are applicable to all the governance and risk management measures described in the Opinion, including the transparency and explainability section. Moreover, the examples mentioned in former

			paragraph 3.25 are not exhaustive. Finally, the Opinion notes that adequate redress mechanisms (e.g. procedures to submit complaints) should also be in place to enable customers to access and seek redress when they have been harmed by an AI system.
201	European Financial Congress	EIOPA's opinion rightly emphasizes that decisions made by AI systems should be understandable to both customers and regulators. However, in practice, ensuring an adequate level of transparency and explainability is particularly difficult with complex models, such as deep neural networks (deep learning) or machine learning models with a large number of parameters and non-linear relationships. Models based on deep learning often act as "black boxes," making it difficult to clearly explain why a particular decision was made. At the same time, customers expect simple, easy-to-understand explanations, while oversight requires more detailed and technical transparency. Requirements for full explainability can lead to significant cost increases and reduced innovation, especially in the insurance sector, where AI is used for complex risk assessments and pricings. We propose to consider the following elements and measures : 1. Alternative measures of explainability at the process level rather than the model level - Rather than requiring full transparency of the model's operation (which is sometimes impossible or very costly), explanations can be provided of the entire decision-making process, such as what data are used, what criteria are considered, what are the stages of verification and human supervision. - This approach allows the customer to understand the decision and supervision without revealing the technical details of the model.	Noted. The Opinion explains that the risk-based approach and the proportionality principle are applicable to all the governance and risk management measures described in the Opinion, including the transparency and explainability section. The proposed elements and measures are in line with the guidance provided in the Opinion in the transparency and explainability section.

		2. Tailor the depth of explanation to the level of risk and the recipient - Models with low risk to the customer may require only basic, simple explanations. - Differences in the level of knowledge of the audience should be taken into account - explanations for the client should be understandable while they may be more technical for supervision. 3. Promote explainable AI (XAI) tools available on the market - In recent years, a number of XAI tools and frameworks (e.g., LIME, SHAP, Anchors) have been developed to generate local and global explanations of the performance of AI models. - It is worth promoting their use in the insurance industry, adapting the tools to the specifics of the data and models. - However, it is important to remember that these tools have limitations and cannot always provide full transparency, especially for very complex models. 4. Implementing the “explainability by design” approach - Already at the design stage of AI systems, the requirements of explainability should be taken into account, choosing models and methods that allow better interpretability (e.g., rule-based models, decision trees, hybrid models). - This approach allows to avoid a situation where an effective but opaque model is difficult to implement due to regulatory requirements. 5. A combination of explainability and human oversight - In cases where model explainability is limited, it is recommended that human oversight of AI decisions be strengthened, which can compensate for the lack of full transparency.	
202	European Confederation of Institutes of Internal Auditing	-The requirements for explainability depend significantly on the model. Some models, like decision trees, are inherently explainable. What additional measures are needed? As mentioned in Section 3.25, there are other explainability approaches like LIME (Local	Noted. The content of transparency and explainability section of the

		Interpretable Model-agnostic Explanations) and SHAP (SHapley Additive exPlanations), as well as reperformance and post hoc explanations.	Opinion is in line with this comment.
203	Federation of European Risk Management Associations (FERMA)	FERMA agrees with EIOPA's opinion on this issue – transparency and explainability are essential requirements for the deployment of any AI system capable of affecting customers interests. As previously mentioned, our view is that insurance undertakings should make sure to inform their customer when an AI system is used as a part of a product or a service, what the purpose of said AI system is, and how it may influence outcomes affecting the interests of the customer. In practice, we recommend creating user transparency panels showing where automated decisions are made and establishing review committees with authority to modify problematic models. For insurance-specific AI (e.g., risk assessment, fraud detection, claims) undertakings should implement: clear pricing explanations, auditable fraud detection, human review options, bias monitoring metrics, and enhanced consent procedures for sensitive data.	Noted. The Opinion is kept principle-based. More detailed guidance may be developed in the future, for instance for specific uses or issues arising from AI systems mentioned in the comment, where appropriate.
204	BETTER FINANCE	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.	Noted. The Opinion is in line with the proposed approach, namely concerning the need to follow a risk-based and proportionate approach, the need to tailor the explanations to the recipient stakeholders and to different uses of AI systems, the important that relevant staff received appropriate trainings, and concerning redress mechanisms.

		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.	
205	Actuarial Association of Europe	Key message: The AAE agrees that explainability is a key principle for the trustworthy use of AI. We support a proportionate and context-sensitive approach to explainability, and recommend clarifying whether this is an obligation of means or results. The Opinion should remain tool-agnostic and avoid singling out specific methods. Broader definitions and expectations for both technical and consumer-facing explainability would support consistency and practicality. Detailed response: We agree with EIOPA that explainability is fundamental to maintaining trust in AI systems and ensuring appropriate governance. However, further clarification is needed on whether explainability is expected as an obligation of results—meaning that AI systems must always be explainable—or an obligation of means, where insurers are expected to make reasonable efforts to achieve it. In practice, many models (especially complex or black-box systems) cannot be fully explained. Our members would favour EIOPA taking a clearer stance on this issue, potentially restricting the use of unexplainable models in high-impact contexts. Equally important is the clarity of communication to customers. Paragraph 3.27 rightly emphasises the need for explanations in simple, accessible language. We support the suggestion that AI systems should not be deployed unless they meet this threshold, particularly for customer-facing applications. This principle reinforces consumer protection and aligns with expectations under the Insurance Distribution Directive. The Opinion currently references specific technical tools—LIME and SHAP—as examples of explainability techniques. While illustrative, naming these methods may inadvertently give the impression that EIOPA is endorsing particular tools. We recommend revising the language to remain tool-agnostic, instead referring to "local and global model-agnostic methods," with examples given only in a footnote. This approach avoids prescribing specific methodologies and allows flexibility for firms to choose appropriate tools based on their use case.	Noted. The Opinion recognises that if the complexity of the AI system hinders the full transparency and explainability, the undertaking should put in place, where necessary, complementary risk management measures such as stronger guardrails and increased human oversight. Undertakings should comprehensively secure and test - before release as well as on an ongoing basis - those uses of AI systems that could have a high impact on customers or the solvency of the undertaking. The references to LIME and SHAP have been moved to a footnote to keep the text of the Opinion adaptable to potential future developments in this area, and the text explains that the assumptions and limitations of these tools

		In addition, we propose expanding the language in Paragraph 3.25 to recognise the limitations of explainability tools. These limitations should be clearly documented, including the rationale for method selection and whether any comparative assessments have been conducted. This would enhance transparency and encourage thoughtful application of multiple approaches when feasible. A broader and harmonised definition of explainability would also be helpful. As with fairness, various definitions exist and may lead to different interpretations across jurisdictions. Regulatory convergence on what explainability means—and how it is assessed—would promote consistency across the market. We also suggest recognising that AI explainability differs from traditional IT systems. For traditional systems, a one-to-one mapping from input to output is typical. In contrast, AI systems—especially probabilistic or learning-based models—may require statistical or stochastic explanations rather than deterministic ones. These forms of explanation should be considered appropriate, provided they support meaningful understanding and traceability of outcomes. Lastly, we propose simplifying the language used. For instance, the phrase “meaningfully explainable” could be streamlined, as its interpretation may vary. Clarity and alignment with existing technical and regulatory frameworks would aid implementation.	should be duly documented and addressed. A reference to statistical or stochastic explanations has been added, which should also be duly justified and documented. The Opinion is kept principle-based, and its content and terminology used is consistent with similar references in sectoral legislation as well as in other regulations such as the GDPR or the AI Act (e.g. regarding meaningful explanations). Nevertheless, EIOPA will continue monitoring market developments via different tools in close collaboration with stakeholders, and it envisages to subsequently develop more detailed analysis on specific AI systems or issues arising from the use of AI systems in insurance and provide further guidance, where appropriate.
206	Finance Watch	In addition to providing the consumer with information about the influence of the AI system on the decision using simple, clear and non-technical language, the consumer should also have the right, as pointed out in our answer to Q9, to request human intervention to review decisions (risk assessments and pricing decisions) made by AI systems.	Noted. The Opinion is kept principle-based. More detailed guidance may be developed in the future, for example concerning some

		Moreover, the explanations provided to consumers should also include information about the categories of data used by the AI system to make decisions that have a material impact on consumers. Having this information is key to allow consumers to make informed decisions, including the decision whether there is a need to contest the decision with the insurance provider. Having access to this kind of information is also key in case the consumer needs to seek redress in court for any damage caused by an AI system used by the insurer and needs to prove that the AI system was at fault (e.g. prove that the AI system was discriminatory because it used biased data).	of the use of AI systems mentioned in the comment, where appropriate.
207	Insurance and Pensions - Denmark	Overarching comment on explainability: It should be added that explainability measures should be adapted to the specific AI technology in use and the specific use case. For “classic” machine learning LIME or SHAP are relevant measures. But for some GenAI-uses other measures must be used, as no sole-ly/purely mathematical measurement can be used on all GenAI-cases. For GenAI and similar use cases assessing the results could be a viable option. I.e. GenAI is the most efficient technology to transcribe a phone call al-lowing for high efficiency gains. If a case worker present during the call must approve the transcription and will correct any errors, additional explainability metrics are not needed, as the result itself is verified. This would be the case for any GenAI or AI use, where a case worker or similar has the relevant knowledge to directly assess and approve the result. Allowing “result verification” is central for the use of GenAI and similar techniques. And it is important to allow different explainability ap-proaches for these approaches, as the Opinion would otherwise general-ly disallow the use of GenAI and similar as these technologies that can-not be explained by traditional ML explanation-techniques (i.e. LIME or SHAP). Comment on legal basis: The section cover both IDD and Solvency II delegated regulation which in terms of explainability have very different scopes. IDD targets objec-tive information on insurance products for consumers. Solvency II con-cerns internal information systems.	Noted. The Opinion explains that the risk-based approach and the proportionality principle are applicable to all the governance and risk management measures described in the Opinion, including the transparency and explainability section. Furthermore, the Opinion explains that the explanations need to be adapted to the different uses of AI systems and the to the recipient stakeholders. It is also acknowledged that for certain uses where there are no suitable alternatives, if the complexity of the AI system does not allow for full transparency and explainability, the undertaking should put in place, where necessary, complementary risk

		To ensure clarity it is important to highlight the different scopes and which regulation apply for the listed elements. I.e. Solvency II require-ments cannot be expected to be meaningfully explained to the aver-age/relevant consumer. On the other hand, understandable explana-tions to the average consumers on insurance products, would not be technical enough to satisfy Solvency II requirements. Text specific comments: Point 3.25 (first sentence): “Undertakings should adopt the neces-sary measures to ensure that the outcomes of AI systems can be mean-ingfully explained.“ Comment: We suggest changing wording to ”Undertakings should where relevant adopt the necessary measures […]” in order to allow for sufficient flexibility for undertakings to select relevant measures in ac-cordance with the AI-techniques used. See comment below for further clarification. Point 3.25 (last part): “Supplementary explainability tools such as LIME or SHAP may also be used to explain the inner functioning of complex AI systems, but the limitations of these tools should be duly documented and addressed.” Comment: Consider rewording “limitations” to focus on using tools like LIME or SHAP correctly in the given context instead of listing generic limitations. Alternative wording suggestion: “but the relevant factors and assump-tions when using these tools should be duly documented […]”. Point 3.26 (first sentence): “In application of the principle of propor-tionality, undertakings should adapt the explanations to specific AI use cases.” Comment: Consider rewording “should” to “when necessary” in order to ensure that a proportionality is in fact considered. Point 3.27 (first sentence): “The explanations should also be adapted to the recipient stakeholders.” Comment: A general requirement for explanations to stakeholders on system level does not follow from current regulation. The sentence should be altered to reflect this.	management measures such as stronger guardrails and increased human oversight. Undertakings should comprehensively secure and test - before release as well as on an ongoing basis - those uses of AI systems that could have a high impact on customers or the solvency of the undertaking. The references to LIME and SHAP have been moved to a footnote to keep the text of the Opinion adaptable to potential future developments in this area, and the text explains that the assumptions and limitations of these tools should be duly documented and addressed. The Opinion has clarified that the scope of the insurance sector legislation mentioned therein is not altered, and the principles outlined in the Opinion are applicable to the use of AI systems in insurance within the scope of the Opinion, based on requirements in sectoral legislation, and following a risk based and proportionate approach

		I.e. by changing “The explanations should” to “Where relevant the ex-planations can be adapted”. Point 3.27 (second sentence): “For example, for competent authori-ties and auditors, the undertakings should be able to provide a global and comprehensive explanation about the functioning of the AI system.“ Comment: This does not follow as a general system requirement from current regulation and the sentence above should be reworded/moved.	
208	Wind Tre S.p.A.	It could be envisioned to implement an information system similar to the provisions of the GDPR, where the customer receives automatic and proactive communication, rather than only upon request. Such a system would allow the registration of the customer's consent while transparently explaining the purposes and usage of the data introduced into the AI system. This approach would enhance customer trust and ensure compliance with the principles of transparency and accountability. The measures on explainability must be consistent and proportionate (taking into account the actual risk) with the measures provided for in art. 13 of the AI Act for high-risk systems. Also in this case, it is necessary to describe in more detail the commitments that weigh on providers of AI systems from those that weigh on deployers, so as to allow the appropriate fairness interventions to be carried out by the correct entity that must put them into practice.	Noted. The Opinion is kept principle-based. More detailed guidance such as the one suggested in the comment may be developed in the future, where appropriate. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems and data they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring.
210	ANASF	We agree, it seems clear and effective to us.	Noted.
212	BEUC - The European Consumer Organisation	- BEUC’s position is consumers shall always be informed when an AI system was used to make a decision and offer the right to human intervention. Transparency cannot be the only solution offered but consumers must have the right to a human assessment to avoid discrimination and unfair treatment.	Noted. The Opinion states that the explanations should also be adapted to the needs of different

		- Point 3.24: Article 20 IDD does not only specify that undertakings shall provide the customer with objective information" but also that any contract proposed shall be consistent with the customer's insurance demands and needs. Where AI system issue a contract proposition, transparent information should be provided to consumers to explain the consistency of the contract proposition with the customer's insurance demands and needs. - Point 3.25: BEUC recommends adding that the outcome of AI systems should be explained to consumers in plain and understandable language. This shall include information on the data categories used to make the assessment and how the assessment is made on this data. EIOPA could provide a template for such information so that consumers receive standardised information about AI systems in the insurance sector. - Point 3.26: BEUC is concerned that insurance operators can escape full transparency if the system is too complex. If the AI decision-making is too complex to explain it, the risks are high that also staff from insurance operators (e.g. employees in customer services) do not understand the decision made and cannot provide qualified advice to consumers on the decision made which raises questions as regards the handling of possible discriminatory treatment etc. BEUC hence rejects the exemption from transparency and explainability for complex AI systems. - Point 3.27 Information on AI systems should always be offered to consumers, not just upon request.	recipient stakeholders, and in particular for customers, in addition to being informed that they are interacting with an AI system, upon the customer's request, the should be informed about influence of the AI system on the decision that has a material impact on them. This is complemented with the need to have adequate redress mechanisms (e.g. procedures to submit complaints) to enable customers to access and seek redress when they have been harmed by an AI system. Furthermore, a reference to customer's insurance demands and needs has been added. Following a risk-based and proportionate approach, for certain uses, it may be possible to complement the limited explainability with complementary risk management measures, although it is highlighted that for higher-risk uses of AI system it is particularly important to secure and test the AI system.

			The Opinion is kept principle-based. More detailed guidance may be developed in the future, where appropriate, and following a risk-based and proportionate approach.
213	Spanish Association of Risk Management and Insurance, known as AGERS	PROPOSALS ADDITIONAL TO THOSE ALREADY PROVIDED FOR IN THE EUROPEAN REGULATION ON ARTIFICIAL INTELLIGENCE Labelling of algorithmic decisions Transparency panel for users • Create an accessible digital space where users can visualise: Internal record of automated decisions Certified AI training for users and employees Extended impact assessment on explainability Internal algorithmic review committees 1.Create internal multidisciplinary bodies with ethical and technical review functions for the models in use, with the capacity to: § Issue transparency reports. § Assess emerging risks. § Interrupt or modify the use of models in case of excessive opacity. I. Particularities of the insurance sector in the use of AI The insurance sector is making increasing use of artificial intelligence systems in areas such as:	Noted. The Opinion is kept principle-based. More detailed guidance, such as in relation to the uses of AI systems mentioned in the comments, may be developed in the future, where appropriate, and following a risk-based and proportionate approach.

		• Risk assessment and premium setting (underwriting). • Fraud detection. • Automated claims management. • Customer service through virtual assistants. • Product segmentation and personalisation. These applications can directly affect economic rights, access to essential services or even non-discrimination of policyholders, which requires a high standard of transparency and explainability. II. Adaptation of specific measures 1. Explanation of decisions in pricing processes o Inform the policyholder, in clear language, of the variables that have most influenced the assigned premium, especially when automated predictive models are used. o Include illustrative examples (‘your premium is reduced if...’) to improve understanding of the impact of certain factors. 2. Traceability in fraud detection o Ensure that the systems used to detect suspicious patterns are auditable and that decisions can be reviewed by human personnel. o Include safeguards against false positives that may unfairly affect policyholders. 3. Strengthened right to human review o Establish clear and accessible channels so that users can request a human review of any relevant decision made by AI, especially rejections of coverage or compensation. 4. Algorithmic fairness indicators	

		o Apply internal metrics to assess whether the models present indirect biases based on gender, age, residence or other factors prohibited by anti-discrimination legislation. o Publish fairness reports or include summaries in the company's transparency policy. 5. Consent and informed understanding o When collecting data for model training or automated processes, reinforce informed consent procedures, especially when dealing with health or behavioural data.	
214	AI & Partners	Transparency is key to responsible AI deployment, and the Opinion provides a strong foundation. However, insurers would benefit from further guidance on balancing explainability with model performance. For complex AI models, alternative approaches—such as model-agnostic interpretability techniques like LIME or SHAP—should be encouraged. The Opinion should also specify how insurers should communicate AI decisions to consumers, ensuring clarity without excessive technical detail. Industry-wide transparency benchmarks, including customer-facing explainability scores, could enhance trust. Additionally, promoting open-source AI governance frameworks would encourage best practices while enabling regulatory bodies to refine transparency requirements over time.	Noted. The Opinion acknowledges the trade-off between accuracy and explainability and emphasises the need to follow a risk-based and proportionate approach. The Opinion also includes references to supplementary explainability tools mentioned in the comment. More detailed guidance, such as such as the one proposed in the comment, may be developed in the future, where appropriate, and following a risk-based and proportionate approach.
		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?	
215	Mirko Kraft	Since ‘the ultimate responsibility of the AMSB of insurance companies includes compliance of AI systems and acknowledge that members of the AMSB should possess collectively sufficient knowledge, skills and experience to oversee all AI systems (Art. 40, 41 Solvency II Directive revised)’, the AMSB is also responsible for the AI systems in the insurance company.	Noted. The Opinion is in line with this comment.

216	BIPAR	In general we consider the EIOPA Opinion comprehensive and helpful in this subject matter. We would like to raise attention over the liability aspects of AI use.	Noted.
217	Studio legale Floreani	The effective human oversight of AI systems requires the identification of adequate competencies and the development of structured training pathways for insurance distributors and staff involved in AI use. It is therefore recommended to: Develop e-learning platforms and shared case study repositories. Introduce mandatory, recurring training programmes for relevant personnel.	Noted. The Opinion highlights the need that roles and responsibilities should be defined in policy documents as well as the need to provide appropriate trainings to the relevant staff.
218	AFPA, Austrian Financial & Insurance Professionals Association	Die menschliche Aufsicht ist aus unserer Sicht unabdingbar. KI-Einsatz braucht menschliche Kontrolle und die Verantwortung muss klar zuordenbar sein. Dem Verhältnismäßigkeitsgrundsatz folgend, wird es aber für viele Unternehmen mit schlanker Struktur schwierig, unternehmensintern ein derart hohes Fachwissen aufzubauen. Um zeitgemäß agieren zu können, müssten Unternehmen ab einer zu definierenden Unternehmensgröße die Position eines CISO und jener eines CISA schaffen und besetzen. Insbesondere die noch wenig verbreitete Position des CISA würde einen gewaltigen Entwicklungsschritt für Unternehmen bedeuten. Es wird aber abzuklären sein, wie derartiges Knowhow eventuell durch externe Wissensträger abgedeckt werden kann. Es muss aktuell allerdings durchaus berechtigt bezweifelt werden, dass es flächendeckend ausreichende Ressourcen am Markt gibt. Human oversight is indispensable from our perspective. The use of AI requires human control, and responsibility must be clearly assignable. Following the principle of proportionality, it will be difficult for many companies with lean structures to build such high expertise internally. To act in a timely manner, companies of a certain size would need to create and fill the positions of CISO and CISA. Especially the still relatively uncommon position of CISA would represent a significant development step for companies. However, it must be clarified how such expertise can potentially be covered by external knowledge carriers. It is currently quite justifiable to doubt that there are sufficient resources available in the market.	Noted. The Opinion now specifies that undertakings may decide to create other organisational arrangements that fit their business model, such as outsourcing certain oversight functions.

219	Insurance Europe	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.	Noted. The Opinion states that a risk-based approach and proportionality principle should be applied to all AI governance and risk management measures, allowing for tailored solutions based on the specific use of AI systems. This approach also applies to the balance between human oversight models, such as "Human-in-the-loop" and "Human-on-the-loop". Concerning the AMSB, the Opinion state that its members are responsible for the overall use of AI systems within the organisation, and therefore they need to have sufficient knowledge of how AI systems are used in their organisation and the potential risks. They are responsible for defining and internally communicating the vision and policy towards the development and use of AI systems within the organisation.
221	Lloyd’s Market Association	We generally agree with this section. However, we would exercise caution that any Opinion regarding human oversight does not require such human oversight to be in house. Smaller undertakings which have out-sourced the development of AI tools and models still need to ensure appropriate oversight of such AI, but may have to contract for such oversight	Noted. The Opinion now specifies that undertakings may decide to create other organisational

		expertise by virtue of their being small. Requiring such knowledge and skills in-house would be disproportionate and lead to lack of competition and innovation. Naturally we agree that due to the complexity of AI systems, those monitoring AI and in charge of oversight should have the appropriate training to be able to monitor it effectively, whether they are in house or contracted in. We note that the final sub-paragraph of 3.29 is expressed with the permissive "may," whereas the introductory sentence of the list prior to the beginning of the list uses the mandatory "should". This should be clarified so as to avoid any confusion.	arrangements that fit their business model, such as outsourcing certain oversight functions. The former paragraph 3.29 referred to the possibility of undertakings creating other organisational arrangements that fit their business model, whereas the previous list refers of more established functions and roles, hence the different terms used.
222	European Federation of Financial Advisers and Financial Intermediaries (FECIF)	We fully agree with the statements in this section: human oversight is absolutely essential throughout the entire life cycle of the AI system, through the assignment of roles and responsibilities to the personnel involved. It is also essential to train and prepare the personnel who will be responsible for applying and overseeing the AI system.	Noted.
223	AMICE	We suggest stating explicitly that the expectation on human oversight should be scaled according to the actual impact and risk profile of the specific AI system. In particular, while acknowledging that according to Solvency II the Administrative, Management or Supervisory Body (AMSB) retains the ultimate responsibility for compliance with applicable law, we suggest emphasizing that the AMSB's role should be strategic, framework-oriented and its oversight should primarily focus on AI systems that pose material risks. In its Final Report on the Guidelines on System of governance, EIOPA clarified that the AMSB's responsibilities do not exclude delegation and, thus, this principle should also apply with reference to the AI oversight.	Noted. The Opinion explains that the risk-based and approach and proportionality principle are applicable to all the governance and risk management measures described in the Opinion, including the Human Oversight section.
224	Institute of International Finance	The extensive use of 'should' language throughout this section creates multiple quasi-obligations regarding oversight roles. For example, paragraph 3.29 contains 6 'should's and only one 'may'. We believe this extensive use of quasi-requirements language is inappropriate in an Opinion which purports not to introduce any new requirements. The Opinion appropriately recognizes different governance functions (AMSB, compliance, audit, data protection) that align with existing structures. However, the Opinion should avoid	Noted. As previously explained, the Opinion does not establish a supervisory checklist, but rather it follows a holistic approach to AI governance and risk management anchored in risk-based and

		being overly prescriptive on roles and acknowledge the possibility that, as AI systems become commodified, less intensive engagement by the AMSB members may be warranted. Furthermore, the engagement of the AMSB members should be scaled according to the impact that the AI system has on the customer and the company activity. The proportionality principle should be stated by EIOPA also in this section.2 The corporate Board of an insurance undertaking should be free to delegate routine tasks to management and its important strategic and oversight function should not be 'cluttered' by requirements to focus on particular topics that today are topical such as AI. We suggest that the guidance allow for automated oversight mechanisms for low-risk applications, with human intervention reserved for material decisions or anomalies.	proportionality considerations. The Opinion also explains that the risk-based approach and proportionality principle are applicable to all the governance and risk management measures described in the Opinion, including the Human Oversight section.
225	Gesamtverband der Deutschen Versicherungswirtschaft	The section on human oversight seems to be based on Art. 14 of the AI Act, which relates exclusively to high-risk AI applications. The importance of human oversight is to be recognised in principle. Nevertheless, the opinion should clarify that human oversight at system level is sufficient (human on the loop) and does not need to be implemented for each individual process (human in the loop) in order to enable the automation of processes. The opinion should allow automated oversight mechanisms for low-risk applications, reserving human intervention for major decisions or anomalies. Otherwise, EIOPA will extend the requirements for high-risk AI applications to all AI applications. The differentiation made in the AI Act between different risk levels should remain untouched and it should be made clear that no extension to the non-high-risk AI area is intended. Furthermore, it is not clear why the 'sufficient training' mentioned in 3.30 should constitute an 'additional regulation' to the requirements in Art. 4 of the AI Act. In addition, human oversight in accordance with Art. 14 of the AI Act is a regulation for high-risk AI applications.	Noted. The Opinion has clarified that it does not set out new requirements and does not seek to alter the scope of the AI Act by extending the requirements of the AI Act for high-risk AI systems to all AI systems. The Opinion also explains that the risk-based and approach and proportionality principle are applicable to all the governance and risk management measures described in the Opinion, including the Human Oversight section. The Opinion states that a risk-based approach and proportionality principle should be applied to all AI governance and risk

			management measures, allowing for tailored solutions based on the specific use of AI systems. This approach also applies to the balance between human oversight models, such as "Human-in-the-loop" and "Human-on-the-loop".
226	CNP Assurances	We suggest clarifying expectations for staff training, the roles of different functions in oversight, and how the "human in the loop" principle should be applied in practice. With respect to paragraph 3.30, clarification could be provided by indicating that staff training and competency requirements should be tailored to the role of the individual and the potential impact of the AI system. A one-size-fits-all approach may not be sufficient, especially when supervisory responsibilities vary widely The potential overlap between roles should also be further clarified. Where permitted, expectations regarding separation of roles or safeguards should be stated. More broadly, we support that the governance of AI is not entrusted to the technical teams but to the general management and the company. Regarding paragraph 3.29, the role of compliance in its control functions, and the conditions for its intervention, should be clarified, taking into account the following principles: These functions must be integrated as early as possible in the development/deployment processes of AI systems. These functions provide advice and guidance to inform the Directorate's decision. Compliance features do not "ensure" that the use of AI system within the organization is compliant. The same principles apply to the DPO: The DPO, as an "independent" function, analyses the compliance of the envisaged system with the GDPR and advises the Management by formulating opinions and recommendations.	Noted. The Opinion states that a risk-based approach and proportionality principle should be applied to all AI governance and risk management measures, allowing for tailored solutions based on the specific use of AI systems. This approach also applies to the balance between human oversight models, such as "Human-in-the-loop" and "Human-on-the-loop". The reference to training has been adapted to reflect that sufficient training should be provided to relevant staff adapted to their respective roles and responsibilities to ensure that the human oversight of AI systems can be effective.

		To promote clarity of roles, it would be appropriate to expand the list of responsibilities to include the participation of other functions in the model governance policies. In paragraph 3.29, among the functions in charge of the supervision of AI systems, the CISO function could be added, the extension of the paragraph would make the supervision of AI systems more inclusive. We would also add that the implementation of AI systems on subjects involving the processing of personal data must also be taken into account in the Data Protection Impact Assessments carried out under the GDPR on such processing.	The importance has been stressed of clearly setting out the roles and responsibilities of different staff and the interplay between them. The Opinion is kept principle-based; more detailed guidance, such as concerning the specific process and roles mentioned in the comment, could potentially be developed in the future, where appropriate.
227	IRSG	We support EIOPA's emphasis on human oversight as a key principle in the governance of AI systems. However, doubts arise in relation to the role that the AMSB members of the insurance company should have in relation to the use of AI systems within their company. Sect. 3.29 states, on one hand, that 'Administrative, management or supervisory body (AMSB) members should be responsible for the use of AI within the organisation and they need to have sufficient knowledge of how AI is used in their organisation and what are the potential risks. They should be responsible for defining and internally communicating the vision and policy towards AI within the organisation'. On the other hand, it states that 'The undertaking may decide to create other organisational arrangements, such as appointing an IA officer which provides oversight and advice to all functions, or creating an IA or data committee which comprises members with the necessary expertise and ensures coordination'. In determining the scope of responsibility for the use of AI in its organisation, sect. 3.29 seems to refer to the use of AI in general, without any distinction. Some IRSG members consider this approach of the Opinion to be excessive, with the following reasoning: 'While AMSB members should be responsible of the overall information systems and ICT risk management and, thus, informed about AI risks that materially affect the company, their role should remain strategic, focusing on AI systems that impact the company's risk exposure or the clients. As currently drafted, sect. 3.29 may suggest that	Noted. The Opinion also explains that the risk-based approach and proportionality principle are applicable to all the governance and risk management measures described in the Opinion, including the Human Oversight section More specifically, the Opinion states that Administrative, management or supervisory body (AMSB) members are responsible for the overall use of AI systems within the organisation, and need to have sufficient knowledge of how AI systems are

		AMSB members should oversee all AI systems, regardless of their risk level or business significance. In reality, many AI applications, such as document processing, do not pose material risks that require direct AMSB involvement. In this respect, it is worth noting that neither DORA nor Solvency II mandate a direct AMSB oversight over any IT systems or tool'. On the contrary, other members of the IRSG consider that it is not appropriate to make such a restriction, since 'the ultimate responsibility of the AMSB of insurance companies includes compliance of AI systems and acknowledge that members of the AMSB should possess collectively sufficient knowledge, skills and experience to oversee all AI systems (Art. 40, 41 Solvency II Directive revised)'. The fact is that Articles 40 and 41 of Solvency II are not sufficiently specific for it to be possible to simply derive from them an obligation on the board members to be aware of each AI system used by the company. On the other hand, art. 4 AI Act establishes a general principle and does not impose knowledge of specific AI systems or obligations on specific persons. It is also true that EIOPA's own Opinion in sect. 3.29 states that 'The undertaking may decide to create other organisational arrangements, such as appointing an AI officer which provides oversight and advice to all functions, or creating an AI or data committee which comprises members with the necessary expertise and ensures coordination'. This seems to imply that it does not expect all members of the management body to have sufficient AI literacy, hence the suggestion that a specific one (or a committee) may be appointed who does. At the same time we experience examples where this is an operational arrangement that is sufficient when it comes to establish efficient social dialogue and employee involvement. But this also seems to be inferred from the fact that, in contrast to other recommendations in this Opinion, where 'should/have to/need to' is used to indicate the measures that should be followed by companies, here it is simply proposed ('may'). Given the relevance of this issue, it should be clarified in this Opinion whether the knowledge of the AI systems used by the company extends to all of them, whether they are used only internally or not (having impact or not on the company, their employees and its clients), and whether it affects all members of the management body, regardless of the fact that all of them assume responsibility by virtue of their position, which is not discussed. On the other hand, in relation to the responsibilities imposed on the company's Data Protection Officer (also sect. 3.29), it should be noted that small undertakings might not have sufficient financial resources to appoint a full-time AI officer or Data Protection Officer. Therefore, outsourcing of these roles should be addressed in order to ensure some professional standards in the sub-contractors. In addition, another option for small	used in their organisation and the potential risks. They are responsible for defining and internally communicating the vision and policy towards the development and use of AI systems within the organisation. The former paragraph 3.29 referred to the possibility of undertakings of creating other organisational arrangements that fit their business model, whereas the previous list, including the AMSB, refers of more established functions and roles, hence the different terms used.

		businesses could be to appoint new board members with significant knowledge in AI, as proposed in this Opinion for undertakings in general (sect. 3.29).	
228	CRO Forum	In paragraph 3.29, the Opinion should reiterate that internal controls systems should be proportional to the risk exposure from the AI systems use. And the level of oversight should be scaled according to the risk exposure. We suggest that the Opinion allows for automated oversight mechanisms for low-risk applications, with human intervention reserved for material decisions or anomalies. Roles and responsibilities for controls should be defined, but don't necessarily need to be in a 'policy' document as the Opinion states. 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 organization. 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. It should be made clear that an AI Officer and AI Committee are not always required, as their inclusion in the Opinion might imply to supervisors that this is mandatory. In point 3.30. while we support the need for training for relevant staff for model oversight, some recognition could be made here that humans making or overseeing complex decisions from an AI System are also prone to errors and biases making them no less fallible than an AI System. In paragraph 3.31, human oversight cannot remove possible bias, but it can reduce the likelihood (see point above).	Noted. The Opinion also explains that the risk-based approach and proportionality principle are applicable to all the governance and risk management measures described in the Opinion, including the Human Oversight section. More specifically, the Opinion states that Administrative, management or supervisory body (AMSB) members are responsible for the overall use of AI systems within the organisation, and need to have sufficient knowledge of how AI systems are used in their organisation and the potential risks. They are responsible for defining and internally communicating the vision and policy towards the development and use of AI systems within the organisation. The Opinion does not state that an AI Officer and AI Committee are always required, providing

			flexibility to undertakings in this regard. The Opinion has clarified that training should be provided to the relevant staff adapted to their respective roles and responsibilities, and that Human oversight by the relevant staff should support the identification and mitigation of potential biases.
229	European Financial Congress	The requirement for human supervision should be proportional to the risk and level of autonomy of AI. Additionally, we note that: - Full inclusion requirements should only apply to AI systems with a significant impact on customers, the company's operations or its financial stability. - The AMSB should be informed and involved only for AI implementations of strategic importance or high risk. We also note that integrating the management of AI systems into the management system and risk management system to the extent indicated by EIOPA will require a significant expansion of staff competencies and hiring of specialists, whose costs are high and availability in the market is limited.	Noted. The Opinion explains that the risk-based approach and proportionality principle are applicable to all the governance and risk management measures described in the Opinion, including the Human Oversight section. Concerning the AMSB, the Opinion explains that tis members are responsible for the overall use of AI systems within the organisation, and need to have sufficient knowledge of how AI systems are used in their organisation and the potential risks. They are responsible for defining and internally communicating the vision

			and policy towards the development and use of AI systems within the organisation.
230	European Confederation of Institutes of Internal Auditing	There need to be specific measures to protect models from attacks based on risks. ‘”The compliance and audit functions should ensure that the use of AI systems, within the organisation is compliant with all applicable laws and regulations” (3.29). It is not the responsibility of the control functions (2d & 3rd line) to ensure compliance. It is the responsibility of the 1st line functions, otherwise, at least for internal audit, there would be a lack of independence. The proposed wording could be changed to “the compliance and internal audit functions should verify, following a risk based approach, that the internal control systems on the AI systems within the organisation, are aligned with all applicable laws and regulations”	Noted. The wording of the Opinion has been amended to reflect that the compliance and audit functions verify that the use of AI systems within the organisation is compliant with all applicable laws and regulations.
231	Federation of European Risk Management Associations (FERMA)	The risk management function responsibility is to support the administrative, management or supervisory body (AMSB) members by (i) comprehensively mapping the different AI systems used throughout the undertaking and their use cases; (ii) assessing the risks associated with each use case and steps in the life cycle on a given AI system; and (iii) mapping the risk prevention and mitigation measures put in place. This is necessary in order to provide AMSB members with an accurate view of the actual AI-related risk exposure of the undertaking. For this reason, risk managers should be involved in any AI or data committee established in an undertaking for the purpose of overseeing AI systems. A designated AI Officer should operate independently, report to upper management, and coordinate with compliance, DPO, actuarial function, and CISO. Moreover, undertakings must integrate AI risk analysis with existing compliance frameworks This must be accompanied by comprehensive staff training and audit plans to address issues of bias detection, transparency, and regulatory compliance throughout the AI lifecycle.	Noted. EIOPA acknowledges that the risk management function and the Chief Information Security Officer (CISO) may also play an important role in the context of AI systems in some organizations, they have not been explicitly referenced in the Opinion, since in line with its principles-based and proportional approach, it focuses on those roles and functions that play a more prominent role. Moreover, the Opinion also acknowledges that the compliance and audit functions verify that the use of AI systems within the organisation is compliant

			with all applicable laws and regulations.
232	BETTER FINANCE	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.	Noted. The Opinion highlights the responsibility of the AMSB for the overall use of AI systems within the organisation, and it has clarified that the trainings should be provided to the relevant staff. The Opinion also foresees the possibility of outsourcing certain functions (not the responsibility).
233	Actuarial Association of Europe	Key message: The AAE supports the inclusion of human oversight as a fundamental principle of AI governance. We suggest clarifying expectations on staff training, the roles of different functions in oversight, and how the "human-in-the-loop" principle should be applied in practice. Greater emphasis on Board responsibility and more precise language around function-specific roles would strengthen this section.	Noted. The Opinion states that a risk-based approach and proportionality principle should be applied to all AI governance and risk management measures, allowing for tailored solutions based on the

		Detailed response: We welcome EIOPA's emphasis on human oversight in the governance of AI systems, particularly those with customer impact. We strongly support the inclusion of a "human-in-the-loop" principle, which is essential to preserving individuals' rights to challenge or understand automated decisions. Effective oversight depends on ensuring that Boards and senior management have the necessary skills to understand and challenge AI deployments. This may require targeted training, recruitment of personnel with relevant experience, or use of external support. We suggest that EIOPA encourage Boards to demonstrate how they are equipping themselves to meet this oversight responsibility. Similarly, Section 3.30 could be enhanced by stating that staff training and competency requirements should be tailored based on the individual's role and the potential impact of the AI system. A one-size-fits-all approach may not be sufficient, especially where oversight responsibilities vary significantly. We agree with the need for sufficient staff training before deployment of AI systems. This should be a precondition for use, particularly in high-impact contexts. Elaborating this point more explicitly would reinforce its importance. Some of our members have questioned whether the establishment of a distinct "AI function" is necessary. We suggest clarifying that existing key functions—such as the risk management, actuarial, or compliance functions—may be equipped to address AI-related issues where appropriate. AI should be seen as a methodological enhancement, not necessarily a structural shift in governance. Nonetheless, where AI has cross-cutting impact, coordination across functions remains essential. In that context, it might be helpful to acknowledge that actuaries may be well-suited to support or contribute to AI-related oversight roles, given their skills in data analysis, risk management and regulatory compliance. This could include supporting the responsibilities of a designated AI Officer or contributing to cross-functional AI committees, where established. Their involvement may help ensure that actuarial and technical considerations are appropriately reflected in the governance of AI systems. We also suggest clarifying the potential overlap between roles. For example, can the	specific use of AI systems. This approach also applies to the balance between human oversight models, such as "Human-in-the-loop" and "Human-on-the-loop". The Opinion has clarified that training should be provided to the relevant staff adapted to their respective roles and responsibilities, and that human oversight by the relevant staff should support the identification and mitigation of potential biases. The Opinion acknowledges that undertakings may decide to create other organisational arrangements that fit their business model, such as an AI Officer, but it is not considered a hard requirement at this stage since as mentioned in the comment and in the Opinion other relevant staff, including actuaries, may be equipped to address AI-related risks and opportunities.

		responsibilities of an AI function be held by the same individual as the Data Protection Officer? Where this is permitted, expectations around role separation or safeguards should be stated. More generally, we propose further emphasis on the accountability of all business functions and the Board for assessing the impact of AI within their respective domains. This holistic perspective reinforces the idea that AI governance is not confined to technical teams but is a firm-wide responsibility. To support role clarity, we propose expanding the list of responsibilities noted under the actuarial function (in Paragraph 3.29) to include the function's involvement in model governance policies. This would better reflect the broader oversight role actuaries play beyond pricing and reserving. Finally, in Paragraph 3.31, the wording around bias mitigation could be improved. We recommend simplifying "contribute to the removal of possible biases in line with the policy of the undertaking" to: "contribute to the removal of biases, consistent with the undertaking's governance framework." This makes the guidance clearer and more action-oriented.	Moreover, the Opinion also specifies that roles and responsibilities of different staff and the interplay between them should be clearly defined.
234	Finance Watch	Another measure that should be considered are human reviews of risk assessments and pricing carried out by AI systems deployed by insurers. Human reviews of automated decisions generated by AI systems can be an important mitigant against inaccurate and biased decisions made by AI systems that can lead to mis-selling and/or financial exclusion. For this reason, a consumer survey conducted by the European Consumer Organisation (BEUC) shows that European consumers agree or strongly agree that AI users should have the right to say "no" to automated decision-making (BEUC, Artificial Intelligence: what consumers say, https://www.beuc.eu/sites/default/files/publications/beuc-x-2020-078_artificial_intelligence_what_consumers_say_report.pdf, 2020). Thus, the Opinion should also include a right for consumers to request human intervention to review decisions made by AI systems.	Noted. In line with the Impact Assessment, the Opinion is kept principle-based. More detailed guidance, for instance in relation to the use of AI systems mentioned in the comment, may be developed in the future, where appropriate.
235	Insurance and Pensions - Denmark	General comment 1: We strongly recommend, that it is also mentioned that human oversight can happen at system level (human on the loop) and does not need to be implemented for every single-run process (human in the loop). I.e. for an automation-purposes a human on the loop can be sufficient with relevant logging and in combination with i.e. flagging of irregularities. The Opinion should clearly reflect, that where relevant (in relation to proportionality and risk)	Noted. The Opinion states that a risk-based approach and proportionality principle should be applied to all AI governance and risk management measures, allowing for tailored solutions based on the specific use of AI systems. This approach also applies

		a human can do oversight on the overall flow instead of assessing every single-run process. General comment 2: A requirement for human oversight on system level (for every use case) does not follow directly from current regulation. For clarity it should be considered to address, that regulation in itself does not require human oversight. That being said Human Oversight will be a very relevant risk mitigation tool when using AI and will be relevant in a risk management scenario addressing i.e. Solvency II requirements. But in our opinion human oversight cannot be interpreted as a general requirement. For clarity this should be addressed in the Opinion.	to the balance between human oversight models, such as "Human-in-the-loop" and "Human-on-the-loop". The Opinion has clarified that the scope of the insurance sector legislation mentioned therein is not altered, and the principles outlined in the Opinion are applicable to the use of AI systems in insurance within the scope of the Opinion, based on requirements in sectoral legislation, and following a risk based and proportionate approach.
236	Wind Tre S.p.A.	It could be proposed to establish a framework of administrative liability for failure to supervise the autonomy of artificial intelligence systems. Such a framework could calibrate the degree of responsibility to reflect the specific circumstances, ensuring that the insurance company is not automatically deemed the sole or objectively liable party. This approach would help avoid stigmatizing or unfairly burdening the company, promoting a balanced allocation of accountability that considers the broader ecosystem of AI deployment and oversight. The measures on human oversight must be consistent and proportionate (taking into account the actual risk) with the measures provided for in art. 14 of the AI Act for high-risk systems. Also in this case, it is necessary to describe in more detail the commitments that weigh on providers of AI systems from those that weigh on deployers, so as to allow the appropriate fairness interventions to be carried out by the correct entity that must put them into practice.	Noted. The Opinion explains that the risk-based approach and the proportionality principle are applicable to all the governance and risk management measures described in the Opinion, including Human Oversight. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems and data they use, even if provided by third parties, and should take steps to ensure proper

			governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring.
238	ANASF	We fully agree with the statements in this section: human oversight is absolutely essential throughout the entire life cycle of the AI system, through the assignment of roles and responsibilities to the personnel involved. It is also essential to train and prepare the personnel who will be responsible for applying and overseeing the AI system.	Noted.
240	BEUC - The European Consumer Organisation	- BEUC recommends referencing in addition the report from EIOPA's Consultative Expert Group on Digital Ethics in insurance as the report provides valuable insights on human oversight. - BEUC's position is consumers shall always be informed when an AI system was used to make a decision and offer the right to human intervention. Transparency cannot be the only solution offered but consumers must have the right to a human assessment to avoid discrimination and unfair treatment. - Point 3.29: To ensure that consumers can receive high-quality advice on their insurance products and receive adequate information about their contracts, it would be key that staff working in customer services and claim handling and complaint units have comprehensive knowledge about the AI system and can accurately deal with cases (e.g. refusal of a contract based on AI decision). Staff in customer services, claim handling and complaint units have to possess necessary decision-making powers to overrule a decision made by AI. Otherwise, consumers will just receive the answer like "The decision was made by AI which we do not have any insights on and which decision we cannot overrule" by those consumer facing services. - Point 3.31 Guardrails mentioned should include that staff of insurance operators can overrule an AI decision to remedy unfair treatment/violation of consumer rights.	Noted. The report from EIOPA's Consultative Expert Group on Digital Ethics in insurance is mentioned in footnote 8 of the Opinion, and more prominently in the Annex. The Opinion also recognises that adequate redress mechanisms (e.g. procedures to submit complaints) should also be in place to enable customers to access and seek redress when they have been harmed by an AI system. Moreover, a reference to escalation procedures has also been included in the Opinion.
241	Spanish Association of Risk Management and Insurance, known as AGERS	In addition to complying with applicable regulations, organisations must carry out risk analyses as required by their various management systems or compliance and data protection programmes. In the case of personal data protection, a risk assessment concerning the rights and freedoms of natural persons must be conducted. All of this is intended to ensure consistency and alignment with the management systems or programmes that may already be in place within the organisation.	Noted. EIOPA acknowledges that the risk management function and the Chief Risk Information Officer (CRIO) may also play an important role in

		The role of the Chief Information Security Officer (CISO) is fundamental, given their strategic and technical responsibilities in safeguarding the organisation's digital assets. Risk management relating to AI-based technologies must be incorporated, and the CISO should play a key role in adopting the strategy, leading the evaluation of security tools and techniques, and overseeing training and awareness initiatives. Accordingly, the compliance function, the Data Protection Officer, the actuarial function, and the CISO must be aligned. The designated collegiate body, or the individual appointed to assume the role of Artificial Intelligence Officer, must ensure that the required obligations and controls are duly implemented. This person shall be appointed by the governing body. To avoid delays, it is recommended that a natural person be designated as the AI Officer to act as coordinator within the collegiate body. The collegiate body or the individual appointed as the AI Officer must operate with full independence and autonomy, reporting directly to the administrative body. They shall be responsible for oversight and advisory duties, must participate in AI-related risk analysis, and act as guarantor that internal AI policies are designed and implemented in accordance with principles of transparency, accountability, and respect for fundamental rights. These policies must be coherent with the organisation's Code of Conduct and other existing management systems. A specific legal framework should be established for the role of the AI Officer. The AI Officer's function shall be supervisory and advisory in nature, ensuring compliance with applicable regulations, and must possess sufficient technical expertise. 3.30 Adequate training must be provided to staff in order to ensure effective human oversight. A training and awareness plan should be developed and coordinated with the Data Protection Officer, the Chief Information Security Officer, and the compliance function. 3.31 A monitoring and audit plan must be established to cover the entire lifecycle of the AI system.	the context of AI systems in some organizations, they have not been explicitly referenced in the Opinion, since in line with its principles-based and proportional approach, it focuses on those roles and functions that play a more prominent role. The Opinion also acknowledges that undertakings may decide to create other organisational arrangements that fit their business model, such as an AI Officer, but it is not considered a hard requirement at this stage other relevant staff may be equipped to address AI-related risks and opportunities.

		Mechanisms must also be developed to identify the origin of both technological and human supervisory bias, ensure its correction, promote transparency and explainability, embed participation and diversity in AI governance teams, appoint a dedicated AI Officer, design training plans and awareness initiatives, and ensure the application of ethical guidelines and compliance with relevant regulations.	
242	Chika Okoli	Contractual AI Risk Monitoring and Oversight clauses among CTPs: Similar to the DPIA for GDPR, direct and indirect AI use via CTPs calls for risk evaluations before and during deployment. In my view there ought to be a demand for insurers to embed AI oversight into contractual arrangements to ensure key elements of the AI system are within acceptable risk thresholds and that material changes are highlighted for review i.e. the automation degree, data sourcing, training/decisioning model etc.	Noted. Concerning third parties (including CTPs) the Opinion clarifies that undertakings are responsible for the AI systems and data they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring.
243	AI & Partners	Human oversight is a crucial safeguard, and the Opinion outlines clear expectations. However, insurers may require more practical guidance on defining AI governance roles and responsibilities. Encouraging the adoption of AI Ethics Committees or AI Risk Officers within insurance firms could enhance accountability. Regular training for employees involved in AI decision-making should be a regulatory expectation, ensuring oversight remains effective as AI evolves. Additionally, the Opinion should highlight the need for clear escalation procedures, allowing human reviewers to intervene in AI-driven decisions when necessary. Case studies on best practices for human-in-the-loop oversight could support implementation.	Noted. The Opinion acknowledges that undertakings may decide to create other organisational arrangements that fit their business model, such as an AI Officer or Ethics Committees, but it is not considered a hard requirement at this stage other relevant staff may be equipped to address AI-related risks and opportunities. The Opinion states that a risk-based approach and proportionality principle should be applied to all AI

			governance and risk management measures, allowing for tailored solutions based on the specific use of AI systems. This approach also applies to the balance between human oversight models, such as "Human-in-the-loop" and "Human-on-the-loop". The Opinion also clarifies that highlights the importance of providing training to the relevant staff.
		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?	
244	BIPAR	We refer to existing rules in this respect and to our above comments.	Noted.
245	Studio legale Floreani	As clarified in Article 2(3)(e) of DORA, not all insurance distributors fall within its scope. Nonetheless, where AI systems are used within the distribution chain, equivalent standards of accuracy, resilience, and cybersecurity should apply to avoid systemic vulnerabilities. Clarification is needed on: The minimum expectations for distributors not directly subject to DORA. The implementation of appropriate safeguards to prevent ICT and operational risks stemming from AI usage.	Noted. The Opinion has clarified that the scope of the legislation mentioned therein is not altered, and the principles outlined in the Opinion are applicable to the use of AI systems in insurance within the scope of the Opinion, based on requirements in sectoral legislation, and following a risk based and proportionate approach.
246	AFPA, Austrian Financial & Insurance	KI muss zuverlässig und sicher sein. Anforderungen an Genauigkeit und Cybersicherheit sind richtig, aber proportional zum Einsatzgebiet umzusetzen.	Noted. Indeed the risk-based and proportionate

	Professionals Association	Wie bereits unter Frage 3 ausgeführt, wird hier die synergetische Bearbeitung mit DORA unabdingbar sein. Ein praktikables Zusammenwirken der verschiedenen Aufsichtsbehörden ist eine Voraussetzung. Es darf hier nicht mit zweierlei Maß gemessen werden. AI must be reliable and secure. Requirements for accuracy and cybersecurity are correct but should be implemented proportionally to the area of application. As already stated under question 3, synergistic processing with DORA will be indispensable here. Practical cooperation between the various supervisory authorities is a prerequisite. There must not be double standards.	approach also applies to this section of the Opinion, EIOPA will monitor the market and legislative developments, including the implementation of DORA (e.g. regarding critical third party service providers) in close cooperation with other authorities.
248	Insurance Europe	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.	Noted. The Opinion has clarified that undertakings should use metrics, including, where appropriate, fairness metrics, to measure the performance (e.g. accuracy, recall etc.) adapted to the AI system in question. Moreover, a cross-references has also been made to the paragraph in the Opinion that addresses the issue of third-party service providers (which often provide Generative AI systems). Furthermore, the holistic approach to AI governance and risk management of the Opinion is also applicable in this section. Finally, as previously mentioned the Opinion has

			clarified that the scope of the insurance sector legislation mentioned therein is not altered, and the principles outlined in the Opinion are applicable to the use of AI systems in insurance within the scope of the Opinion, based on requirements in sectoral legislation, and following a risk based and proportionate approach.
250	Lloyd's Market Association	We generally agree with paragraph 3.33 that the levels of robustness and cyber security should be proportionate to the nature, scale and complexity of the AI system. Undertakings should take reasonable steps to ensure that systems are accurate and perform consistently. However, like any process, system or workflow unreasonable expectations of zero failure, or 100% consistency are misplaced. In particular, smaller insurers may have to rely on third-party models as they do not have the resources or expertise in house to develop their own model or tools. These entities may lack direct control within the AI model and its functions. When compared to a large insurer who operates their own in-house AI model this would put the smaller insurer at a disadvantage and could lead to a lack of competition. Outsourcing to specialist providers of AI systems, Infrastructure and Cyber Security should therefore not be discouraged by overly onerous requirements for in-house knowledge and expertise. However, we reiterate our comments in the prior section that smaller insurers that outsource still need to ensure appropriate oversight of such AI.	Noted. The risk-based and proportionate approach is also applicable to this section of the Opinion. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems and data they use, even if provided by third parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring.
251	European Federation of Financial Advisers and Financial Intermediaries (FECIF)	Robustness is a prerequisite for IT security, which must be pursued through technical analysis of physical media and their quality, constant updating, and expanding the possibilities for timely intervention in the event of problems or critical issues. To make an IT system impenetrable, it should be isolated. Companies could be advised to 'split' their AI	Noted.

		system, keeping one connected to the network and one stand-alone, thus obtaining additional security protection.	
252	AMICE	We strongly recommend that EIOPA applies the proportionality principle mentioned in this section across all governance and risk management measures mentioned in the Opinion. As we have pointed out with regard to data governance, transparency, documentation, and human oversight, overly broad regulations may not be suitable for AI systems with minimal risks. A consistent focus on proportionality in all regulatory measures would foster innovation while effectively managing risks and ensuring a balanced and efficient governance structure.	Noted. The risk-based and proportionate approach is also applicable to this section of the Opinion.
253	Institute of International Finance	We strongly support that 'The levels of accuracy, robustness and cybersecurity should be proportionate to the nature, scale and complexity of the AI system' (para 3.33). This proportionate approach is essential for practical implementation and should be extended to all governance and risk management measures outlined in the proposed Opinion. The requirement for 'adequate and up-to-date IT infrastructure as well as fall-back plans to ensure ICT business continuity' (para 3.35) appears to duplicate existing cybersecurity requirements and may create parallel obligations. We do not support the need for any additional guidance in this area. We in any case suggest the Opinion recognize evolving standards for AI security testing and auditing, while allowing undertakings flexibility in implementation approaches.	Noted. The risk-based and proportionate approach is also applicable to this section of the Opinion. The high-level reference to fall-back plans and business continuity is in line with sectoral legislation. Some specificities arising from AI systems may need to be considered. EIOPA will monitor the market and legislative developments, including the implementation of DORA (e.g. regarding critical third party service providers) in close cooperation with other authorities.
254	Gesamtverband der Deutschen Versicherungswirtschaft	The characteristic of accuracy should be interpreted differently. The cited Article 46 SII, which is implemented in Germany in § 23 VAG, provides for an effective internal control system, which in turn includes the compliance function. The latter is intended to monitor compliance with the requirements. However, compliance with the requirements is not just 'black and white'; a distinction must be made between '' permitted'' and '' not permitted''. It is therefore necessary to clarify that the accuracy relates solely to the decision between	Noted. The risk-based and proportionate approach is also applicable to this section of the Opinion.

		permitted/not permitted. The term ‘fairness metrics’ in 3.34 is not used in the AI Act, DORA or Solvency II. In order to ensure standardised terminology and prevent misunderstandings, the term should be deleted. In any case, it should be questioned what is meant by ‘fairness’ in legally permitted procedures and who has to decide on this.	The Opinion has clarified that undertakings should use metrics, including, where appropriate, fairness metrics, to measure the performance (e.g. accuracy, recall etc.) adapted to the AI system in question.
255	CNP Assurances	Regarding paragraph 3.32, the reference to the main legal provisions related to the DORA regulation could be supplemented to include other articles dealing specifically with the robustness and cybersecurity of ICTs, such as, Article 6 (on the ICT risk management framework), Article 17 (on the ICT incident management process), Article 18 (on the classification of ICT incidents and cyber threats), Article 19 (on the reporting of major ICT incidents and voluntary notification of significant cyber threats) and finally Article 28 (Chapter 5, on risk management related to ICT third-party service providers). As a reminder, only Article 11 ("Response and recovery") is mentioned in this section. About paragraph 3.33, the criticality of the AI systems regarding the insurance company's activities must also be considered to ensure the proportionality of the robustness and cybersecurity measures (in addition to "the nature, scale and complexity of the AI system"). The concepts of "Risk-based approach" and "Security by design" should be mentioned in this paragraph as essential incoming processes for the implementation of robustness and cybersecurity. The necessary revision of the contractual framework with third-party service providers (DORA and AI Act impacts) could be added to this paragraph. Regarding paragraph 3.34, it only deals with performance-related metrics but does not address cybersecurity metrics. In addition, it could be recommended to correlate performance monitoring metrics with the safety level of AI systems, as an observed degradation in the performance of AI models/systems may indicate a security issue or security event. We suggest that performance measurement needs to be clarified and adapted to generative AI in particular, indeed, talking about accuracy rate, and "Recall" for generative AI seems complicated in view of the very functioning of these AIs: 2 times the same query can give significantly different results, but above all, and reworking the prompt, it is possible to change the result,	Noted. Some additional references to DORA have been included, but it is important to highlight that the legal references to sectoral legislation throughout the document are not exhaustive. Similarly, the Opinion does not provide an exhaustive list of metrics. The Opinion has included a explicit reference to risk-based and proportionate approach. Moreover, a cross-reference has also been made to the paragraph in the Opinion that addresses the issue of third-party service providers (which often provide Generative AI systems). Furthermore, the holistic approach to AI governance and risk management of the

		It also seems appropriate to specify that information on the propensity to memorize the AI systems should be collected before any deployment of an AIS capable of processing personal data. It seems desirable to remember that the robustness of IS security should also be the subject of regular tests. Paragraph 3.35 focuses mainly on "ICT business continuity" (availability), and a reminder of the data integrity and confidentiality objectives as defined in the AI Act – Article 15 (5) could be mentioned. Other security measures and controls could be highlighted to ensure resilience, as "adequate and up-to-date IT infrastructure" primarily addresses the AI system environment. However, the robustness and security of the AI system rely on both (i) a secure AI support infrastructure and (ii) a secure AI system (access control, filtering functions, logging, appropriate tests, etc.). Knowledge of AI-specific threats should also be mentioned as this is a critical point in defining adequate security and resilience. Finally, this paragraph could also mention that the process of managing incidents related to AI systems is subject to both regulations (DORA and AI Act) in case of outsourcing.	Opinion is also applicable in this section. The remaining detailed suggestions have not been added to the Opinion at this stage to keep it focused in line with the Impact Assessment, but they would be taken into account should more detailed guidance was to be developed at a later stage, where appropriate.
256	IRSG	We agree with EIOPA's approach regarding the proportional application of cybersecurity requirements, which takes into account the nature, scale, and complexity of AI systems. This risk-based approach is essential to ensure that regulatory expectations remain both effective and practical, avoiding unnecessary burdens on low-risk AI applications which may hinder their development and application, to the detriment of insurers' competitiveness and consumer welfare. We therefore encourage EIOPA to extend this principle of proportionality to all governance and risk management measures outlined in the Opinion. As we have previously highlighted in relation to data governance, transparency, documentation, and human oversight, broad requirements and expectations may not be appropriate for AI systems that pose negligible risks. Ensuring consistent proportionality across all regulatory requirements would help balance AI innovation with risk mitigation, while maintaining a clear and effective governance framework.	Noted. Indeed the risk-based approach and proportionality principle is applicable to all the governance and risk management measures outlined in the Opinion.
257	CRO Forum	In point 3.33, consideration should be given to the AI system's 'use or purpose' as well as its nature, scale and complexity. Given AI Systems effectively learn and can improve accuracy or, conversely, drift over time, the requirement for an AI System to perform consistently through the life cycle may need to	Noted. The paragraph mentioned in the comments has been slightly amended, and now states that undertaking

		be tempered in point 3.33. Many of the cybersecurity risks associated with AI are not new. Impersonation threats, data poisoning, more sophisticated phishing attacks, data leakage, prompt injection, sensitive information disclosure are all risks that could have a greater impact or likelihood through improper or incomplete safe management of AI Systems. Controls for these risks would largely already be in existence for established, larger or more mature insurers and where appropriate may need to be adjusted to recognise how these risks might crystalise in a firm's increased usage of AI Systems.	should use metrics, including, where appropriate, fairness metrics, to measure the performance (e.g. accuracy, recall etc.) adapted to the AI system in question. These metrics should support ongoing monitoring and enable the timely identification and remediation of issues such as model drift or data degradation.
258	BETTER FINANCE	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.	Noted.
259	Actuarial Association of Europe	We support the inclusion of accuracy, robustness, and cybersecurity as key principles for the governance of AI systems. However, the use of fairness metrics should be approached with caution. These tools may not always reflect real-world fairness and, if applied uncritically, can lead to misleading or counterproductive outcomes. We suggest that the Opinion encourage the use of fairness metrics only where appropriate, and as part of a broader, context-sensitive assessment supported by professional judgement. Further emphasis on robustness over time, including monitoring for model drift and data degradation, and clearer expectations around cybersecurity practices, would also strengthen this section.	Noted. The references to fairness metrics has slightly been amended, and now it refers to their use "where appropriate". A reference to the need to monitor and address data and model drift has been added.
260	Insurance and Pensions - Denmark	The sections references both Solvency II and DORA as legal basis. To avoid unnecessary burdens by extending the scope of these regulations to use cases, that are out of scope, the specific elements/considerations in the section should be clearly marked as to whether they apply in light of DORA or Solvency II. It should also be made clear that use cases that are out of scope of the regulations are not included in the supervisory expectations, and that any recommendations here are purely inspirational. Text specific comments:	Noted. The Opinion has clarified that the scope of the insurance sector legislation mentioned therein is not altered, and the principles outlined in the Opinion are applicable to the use of AI systems in insurance within the scope of the Opinion, based on

		Point 3.33: “The levels of accuracy, robustness and cybersecurity should be proportionate to the nature, scale and complexity of the AI system. The AI system should perform consistently in those respects throughout their lifecycle, regardless of whether they have been devel-oped in-house or purchased from third-party service providers.” Comment: DORA Article 11 (4) & (6) does not set specific cybersecurity requirements for specific systems. Thus “cybersecurity” should be re-moved from the sentence – and could be added as an additional con-sideration. Point 3.34: See suggestion below to add “where relevant” and “relevant” in the sen-tence in order to promote the proportionality and risk based approach: ”The undertaking should [Add: “where relevant”] use metrics, including [Add: “relevant”] fairness metrics, to measure the performance (accu-racy, recall etc.) adapted to the AI use case in question …”	requirements in sectoral legislation, and following a risk based and proportionate approach. Regarding the comment about DORA, the Opinion aims to highlight some of the main aspects that are relevant in the context of AI systems. Concerning the paragraph about metrics, it now specifies that undertaking should use metrics, including, where appropriate, fairness metrics, to measure the performance (e.g. accuracy, recall etc.) adapted to the AI system in question.
261	Wind Tre S.p.A.	The establishment of shared regulatory metrics, together with defined use cases and specific training protocols, centralized and coordinated by the supervisory authority, could create a level playing field among operators. This approach would also provide clients with assurances regarding the transparency and adequacy of the protocols related to artificial intelligence systems. By standardizing practices and fostering alignment across the industry, such measures would enhance trust in AI systems while ensuring compliance with regulatory expectations.The measures on Accuracy, robustness and cybersecurity keeping must be consistent and proportionate (taking into account the actual risk) with the measures provided for in art. 15 of the AI Act for high-risk systems. Also in this case, it is necessary to describe in more detail the commitments that weigh on providers of AI systems from those that weigh on deployers, so as to allow the appropriate fairness interventions to be carried out by the correct entity that must put them into practice.	Noted. The Opinion is kept principle-based. More detailed guidance such as the one suggested in the comment may be developed in the future, where appropriate. Concerning third parties, the Opinion clarifies that undertakings are responsible for the AI systems and data they use, even if provided by third

			parties, and should take steps to ensure proper governance and risk management as relevant, including for instance through contract clauses, audits, and monitoring
262	ANASF	Robustness is a prerequisite for IT security, which must be pursued through technical analysis of physical media and their quality, constant updating, and expanding the possibilities for timely intervention in the event of problems or critical issues. To make an IT system impenetrable, it should be isolated. Companies could be advised to 'split' their AI system, keeping one connected to the network and one stand-alone, thus obtaining additional security protection.	Noted.
264	BEUC - The European Consumer Organisation	- Point 3.33: As flagged previously, “proportionate to the nature, scale and complexity of the AI system” needs to be further defined as otherwise to much leeway is given to insurance operators to make their own proportionality assessment. - Point 3.34: The Fairness metrics established in Annex I should be used as the baseline - Point 3.35: Cybersecurity should not only consider the potential impacts on the AI system of the insurance operator (e.g. data poisoning, disruption of business) but also the risk of storage of large amounts of data in a given location which could be hacked and used for other purposes outside.	Noted. The references to proportionality have now been harmonised across the document, which refers to the need to follow risk-based and proportionate approach. The Opinion includes a section how this should be implemented. The Opinion has clarified that the examples of fairness metrics are not meant to be prescriptive, among other things in view of the ongoing research in this area. The reference to the location of data since too detailed for the purpose of the Opinion.
265	Spanish Association of Risk Management and	1. Accuracy	Noted. The Opinion incorporates similar notions

	Insurance, known as AGERS	AI systems must maintain an adequate level of accuracy throughout their entire lifecycle. The European Commission is responsible for defining the parameters and methodologies that will allow for the objective measurement of such accuracy. Furthermore, this information must be clearly included in the user instructions for each system, ensuring transparency and technical traceability. 2. Robustness The regulation requires that systems be robust against errors and failures, both in their internal functioning and in their interaction with the surrounding environment. To this end, technical redundancy mechanisms, failure prevention plans, and measures to avoid biases arising from continuous learning must be implemented—particularly those that may create undesirable feedback loops. 3. Cybersecurity The regulation prioritises resilience against cyberattacks, stipulating that systems must be able to prevent, detect, respond to, and recover from incidents. Specific threats considered include: • Data and model poisoning • Evasion through adversarial examples • Breaches of confidentiality • Exploitation of model vulnerabilities It is recommended that a dedicated Commission be established to develop appropriate guidelines and recommendations tailored to the various technological risks posed by AI-based systems that may impact the insurance sector. Responsibilities Nothing further to add beyond what is set out in the AI Regulation. • Providers: must ensure compliance with the Regulation, subject their systems to a conformity assessment, and issue the EU declaration of conformity, which includes cybersecurity commitments. • Importers and distributors: are required to verify the system’s compliance and to include the	as those outlined in the comment, but provides a higher-level overview, consistent with the Impact Assessment's suggested guidance.

		relevant documentation before placing it on the market. • End users (organisations): must follow the user instructions, monitor the system's performance, and report any serious incidents.	
		Q11 - Do you have any comments on the possible risks identified for customers and undertakings?	
266	CRO Forum	The CRO Forum are supportive of the intent in the Opinion paper and its impact assessment to promote supervisory convergence, to reflect a risk based and proportional approach. The CRO Forum's work on Risk Management in AI identified similar risks to those outlined in the Impact Assessment. In addition, the CRO Forum also identified risk of: - inaction (i.e. not leveraging the potential of AI), - conversely the risk of over investment (i.e. the risk of solving low value problems with expensive AI solutions), - organisation data leakage (e.g. customer data) or loss of intellectual property (e.g. trade secrets) - external threat actors augmenting and weaponizing their attacks (e.g. high-quality phishing campaigns and new malware code generation) and impacting the integrity of data and the performance of AI systems (i.e. data poisoning). - impacting the environment (through the extraction/treatment of rare metals for chips or the use of power-hungry data centres for the data centres needed for AI Systems), and - societal impacts as those without the skills to work with AI System become increasingly unemployable.	Noted.
267	Actuarial Association of Europe	We strongly support the application of the fairness principle in managing AI risks. Unfair treatment can arise in areas beyond high-risk use cases, such as in automated claims handling and non-life pricing, including natural catastrophe cover. These applications may carry significant consumer and reputational risk. The AAE has previously highlighted the importance of fairness in its 2024 discussion paper on Social Sustainability in Insurance. In addition to consumer harm, unfair AI outcomes can pose financial risks to insurers via litigation and reputational damage, reinforcing the prudential relevance of this principle.	Noted.
268	Finance Watch	We agree with the risks identified but would add the additional risks outlined in our answer to Q1.	Noted.
270	AI & Partners	The emphasis on cybersecurity and AI model robustness is well-placed, but the Opinion could provide more concrete recommendations. Insurers should be encouraged to implement adversarial testing frameworks to assess AI vulnerability to data poisoning and model manipulation. Standardized AI performance monitoring metrics—such as stability, recall, and fairness scores—could enhance risk oversight. Additionally, insurers should maintain fallback mechanisms, ensuring business continuity in case of AI system failures. Greater collaboration with cybersecurity regulatory bodies, such as ENISA, would strengthen sector-	Noted.

		wide AI resilience. Establishing regular AI stress tests could further ensure long-term accuracy and security compliance.	
		Q12 - Do you have any comments on the analysis of costs and benefits?	
271	Studio legale Floreani	A proportionate approach to cost-benefit analysis is essential, particularly in the context of smaller or less complex insurance distributors. Such entities should not be unduly burdened with requirements that compromise their ability to maintain client-centric service and regulatory compliance. The analysis should reflect the role of insurance distributors as key actors in the insurance value chain, ensuring that requirements remain feasible, scalable, and commensurate with the risks involved.	Noted. Indeed the Opinion explains that the risk-based approach and the proportionality principle are applicable to all the governance and risk management measures described in the Opinion, including with regards to insurance distributors.
272	CRO Forum	For the costs of option 1.1/Supervisors, the training costs for supervisors would arguably exist whether there was an EIOPA opinion or not. In addition, many supervisors already have teams capable of overseeing the data, supply chain and model risks that are inherent in AI Systems. For the benefits, of option 1.1/Industry, for international insurers a clear and consistent picture of expectations from European Regulators on the risk management of AI Systems will be beneficial as it will help ensure the requirements for firms for AI risk management from the regulatory bodies remains joined up and non-contradictory. This would help mitigate the risk that, for example, an information or data specific regulator's requirements contradict consumer or prudential requirements in the same jurisdiction.	Noted. The costs analysis has slightly been amended to amend the impact on supervisors. The benefits of supervisory convergence are acknowledged.
273	European Financial Congress	The cost-benefit analysis in the document is rather general and does not fully take into account: - Additional costs resulting from the expanded documentation and monitoring requirements that the Authority imposes over and above the AI Act. - Potential costs associated with the need to adapt IT systems, hire appropriate specialists and train personnel beyond the requirements that the AI Act imposes. - The risk of reducing the competitiveness of the insurance industry, especially in case of smaller entities that may have difficulty bearing such costs. - Interpretativeuncertainty that may force excessive safeguards "just in case," further increasing expenses.	Noted. A reference has been added to the potential impact on insurers competitiveness, although but the impact is expected to be limited given the high-level nature of the Opinion and the fact that undertakings already have to comply with existing insurance legislation.

		It is worthwhile for the cost-benefit analysis to address these aspects, showing the scale and nature of the burden, and the potential consequences for innovation and market competitiveness.	
274	Actuarial Association of Europe	The AAE has no specific comments on the expected costs and benefits at this time. However, we support the principle of proportionality and encourage EIOPA to monitor the practical impact of implementation, particularly for smaller undertakings and in relation to resource-intensive requirements such as documentation and data governance.	Noted.
276	AI & Partners	The Opinion provides a balanced view of the costs and benefits of AI governance in insurance, but further quantification of implementation costs for insurers—especially smaller firms—would be beneficial. Clearer guidance on expected compliance expenditures and potential efficiency gains would support industry adoption. Additionally, incorporating case studies demonstrating cost savings from AI-driven risk management could strengthen the business case for robust governance. While the long-term benefits of responsible AI use are evident, a phased approach to compliance, particularly for mid-sized insurers, could help mitigate short-term financial burdens while ensuring adherence to regulatory expectations.	Noted. The view of costs and benefits has been kept proportionate to the nature of the Opinion.
		Q13 - Do you have any comments on the policy option chosen?	
278	IRSG	We appreciate EIOPA's initiative and its stated objectives. Although most of the AI systems deployed by insurance undertakings are neither prohibited nor classified as "high-risk" by the AI Act, advanced AI applications extensively used in core insurance functions such as underwriting, pricing, and claims management may generate risks that require proper oversight. Further comments see our response to Q 1.	Noted.
279	CRO Forum	The CRO Forum supports the recommendation to develop an Opinion, to support supervisors and insurers on how existing sectorial legislation (e.g. Solvency II, IDD) should be interpreted in the context of the use of AI systems in insurance, with a strong focus on the need to adopt risk based and proportional approaches.	Noted.
280	European Financial Congress	EIOPA's document aptly identifies key risks associated with the use of AI in the insurance sector, such as discrimination risks, lack of transparency in decisions, privacy violations, operational and reputational risks. However: - It should be noted that the diversity of interpretations by national supervisors can lead to inconsistent application of the requirements, which increases legal and operational uncertainty for companies. - EIOPA goes beyond the AI Act requirements by extending risk management expectations also to sysetms that the AI Act does not classify as high risk. - This expansion can result in the imposition of obligations on companies that are not formally mandated by the AI Act, raising the risk of overregulation and increased costs for the insurance industry.	Noted. The Opinion aims to promote a convergent approach to AI governance and risk management, but at the same time it is anchored in a risk-based, principle based and proportionate approach. Furthermore, the Opinion specifies that it does not

			set out new requirements and does not seek to alter the scope of the AI Act by extending the requirements of the AI Act for high-risk AI systems to all AI systems used in insurance.
281	Actuarial Association of Europe	The AAE does not have additional comments on the proposed policy option. We support EIOPA's principle-based and proportionate approach and agree that providing supervisory convergence through non-binding guidance is an appropriate next step.	Noted.
282	Finance Watch	We agree with the analysis that there is an urgent need for policy action, however, we disagree with the proposed approach, as outlined in our answer to Q14.	Noted.
283	Insurance and Pensions - Denmark	We agree with the suggested policy action.	Noted.
285	AI & Partners	The selected policy option aligns with broader regulatory trends and provides a risk-based, proportional approach. However, further clarity on how it compares to alternative regulatory models—such as those in banking or other financial sectors—would be helpful. A deeper examination of whether additional incentives, such as regulatory sandboxes or AI governance certifications, could improve industry adoption would be valuable. Additionally, the policy should consider how insurers can leverage existing governance frameworks under Solvency II and GDPR to avoid redundant compliance efforts. A clearer articulation of why this option was preferred over more prescriptive alternatives would enhance transparency.	Noted. The Opinion is kept principle-based, with some specific and non-prescriptive examples included in the Annex. More detailed guidance may be developed in the future, where appropriate.
		Q14 - Do you have any comments on the proposed approach?	
286	IRSG	We agree on the choice of issuing a high-level opinion addressed to supervisors, instead of detailed guidance addressed to insurance undertakings. Further comments see our response to Q 1.	Noted.
287	CRO Forum	The CRO Forum supports the approach of providing high level guidance on explaining supervisory expectations for the interpretation of legislation in the context of AI systems. Aligning with the high-level principles in the EU AI Act and other international initiatives in this area should reduce overlap or contradictory requirements. The approach of subsuming AI under existing regulatory frameworks, rather than treating it as a special case, has merits in terms of consistency and practicality. Before developing new supervisory frameworks (or the more detailed guidance that is mentioned as a possible next step in the 'approach' section of the paper), careful consideration should be given to whether existing risk management requirements are sufficient.	Noted.

		The EIOPA should continue to consult with the full range of regulatory and statutory bodies to ensure that the requirements for firms for AI risk management from these bodies remains joined up and non-contradictory. This would mitigate the risk that, for example, an information or data specific regulator's requirements contradict consumer or prudential requirements in the same.	
288	European Financial Congress	See answer to Q 13	Noted.
289	Actuarial Association of Europe	We welcome the annexes as a useful practical supplement to the Opinion. In particular, we support the inclusion of examples to guide proportional implementation. To further enhance their usefulness, we suggest incorporating references to established model validation techniques, including quantitative testing methods, robust documentation practices, and indicators of system performance, including, where appropriate, commonly used indicators of model performance (e.g. Precision, Recall, or F1-score), recognising that these should be selected based on the use case and validation objectives. We note that some national approaches, such as the principles outlined by BaFin in Germany, offer similar guidance in relation to data governance and algorithmic decision-making.	Noted.
290	Finance Watch	We disagree with the policy option chosen to only provide high level guidance based on existing legislation. As rightly pointed out in the Impact Assessment, at the time the legislation was approved AI systems did not exist or they were not widely used. Therefore, the existing sectoral legislation (e.g. IDD and SII) that apply to the use of AI in the insurance sector was not drafted with the deployment of AI and its unique risks to consumers in mind. Therefore, high level guidance is not sufficient to adequately protect consumers from the considerable risks AI brings. For the industry, this approach will also result in a lack of legal clarity which in turn could disincentivize investments in AI systems by insurers and cause level-playing field issues. At a bare minimum, detailed guidance on specific use cases or issues (Policy option 2.2) would be required. Having robust safeguards in place to ensure that AI used in retail financial services does not harm consumers are needed to not only ensure consumer protection but also to meet the EU's competitiveness goals. In order for AI to be taken up and financial institutions to be competitive, societal trust in AI and in the wider financial system are needed. Therefore, implementing sufficiently robust regulation of AI and promoting its development and uptake in the EU go hand in hand and must be pursued in parallel and not be seen as being in opposition to each other.	Noted. While the option of providing high level guidance based on existing legislation has been retained, EIOPA envisages to subsequently develop more detailed analysis on specific AI systems or issues arising from the use of AI systems in insurance and provide further guidance, as appropriate.

291	Insurance and Pensions - Denmark	We agree with the proposed approach. AI is a fast-moving technology. Best practice to address challenges can (and will) change quickly. Therefore, a high-level approach which leave flexibility and room for change in order for companies to adapt to their specific setup and busi-ness needs is in our opinion the best way to ensure clarity on require-ments. This will clarify requirements and leave flexibility for the companies to adapt to requirements in the way they see fit.	Noted.
294	AI & Partners	The principle-based, risk-proportionate approach ensures flexibility while maintaining strong governance expectations. However, additional guidance on practical implementation steps—such as standardized risk assessment templates or governance best practices—could aid insurers in compliance. The Opinion could also explore greater alignment with international AI governance frameworks, ensuring consistency for multinational insurers. Furthermore, consideration of industry feedback through pilot programs or regulatory sandbox testing could refine the approach before full-scale implementation. Providing more concrete regulatory expectations for AI fairness, transparency, and explainability would enhance clarity and ensure insurers apply consistent standards in practice.	Noted. While the option of providing high level guidance based on existing legislation has been retained, EIOPA envisages to subsequently develop more detailed analysis on specific AI systems or issues arising from the use of AI systems in insurance and provide further guidance, as appropriate