CONSULTATION PAPER

On Opinion on Artificial Intelligence Governance and Risk Management

EIOPA-BoS-25-007
10 FEBRUARY 2025

European Insurance and
Occupational Pensions Authority

RESPONDING TO THIS CONSULTATION PAPER

EIOPA welcomes comments on the Consultation paper on Opinion on Artificial Intelligence Governance and Risk Management.

Comments are most helpful if they:

- respond to the question stated, where applicable;
- contain a clear rationale; and
- describe any alternatives EIOPA should consider.

Please send your comments to EIOPA via the EU Survey, by 12 May 2025. Contributions not provided via the EU Survey or after the deadline will not be processed. In case you have any questions please contact Aiopinion@eiopa.europa.eu

Publication of responses

Your responses will be published on the EIOPA website unless: you request to treat them confidential, or they are unlawful, or they would infringe the rights of any third party. Please, indicate clearly and prominently in your submission any part you do not wish to be publicly disclosed. EIOPA may also publish a summary of the survey input received on its website.

Please note that EIOPA is subject to Regulation (EC) No 1049/2001 regarding public access to documents and EIOPA's rules on public access to documents[1].

Declaration by the contributor

By sending your contribution to EIOPA you consent to publication of all information in your contribution in whole/in part – as indicated in your responses, including to the publication of your name/the name of your organisation, and you thereby declare that nothing within your response is unlawful or would infringe the rights of any third party in a manner that would prevent the publication.

Data protection

Please note that personal contact details (such as name of individuals, email addresses and phone numbers) will not be published. EIOPA, as a European Authority, will process any personal data in line with Regulation (EU) 2018/1725. More information on how personal data is treated can be found in the privacy statement at the end of this material.

Next steps

EIOPA will consider the feedback received, develop the impact assessment based on the answers to the questions included in this consultation paper, and revise this Opinion accordingly.

[1] Public Access to Documents

EIOPA | Westhafen Tower, Westhafenplatz 1 | 60327 Frankfurt | Germany
Tel: +49 69-951119-20
info@eiopa.europa.eu | https://www.eiopa.europa.eu

1. LEGAL BASIS

1.1. The European Insurance and Occupational Pensions Authority (EIOPA) provides this Opinion on the basis of Article 29(1)(a) of Regulation (EU) No 1094/2010[2]. This Article mandates EIOPA to play an active role in building a common Union supervisory culture and consistent supervisory practices, as well as in ensuring uniform procedures and consistent approaches throughout the Union.

1.2. EIOPA delivers this Opinion on the basis of Articles 17, 20 and 25 of the Directive (EU) 2016/972 (Insurance Distribution Directive),[3] Articles 41, 46 and 82 of the Directive 2009/138/EC (Solvency II Directive),[4] Articles 4, 5, 6 and 11 of the Regulation (EU) 2022/2554 (Digital Operational Resilience Act),[5] Articles 258 and 260 of the Commission Delegated Regulation 2015/35,[6] and Articles 6, 7, 8 and 9 of the Commission Delegated Regulation 2017/2358.[7]

1.3. This Opinion is addressed to the competent authorities, as defined in Article 4(2) of the Regulation (EU) No 1094/2010, and covers the activities of both insurance undertakings and intermediaries (hereafter jointly referred as 'undertakings'), insofar they may use AI systems within their respective areas of competence in the insurance value chain.

2. CONTEXT, OBJECTIVE AND SCOPE

2.1. Artificial Intelligence (AI) is expected to play a pivotal role in the ongoing digital transformation in all industries, including the insurance sector, where there is a trend towards the increasing use of AI systems throughout the insurance value chain.

2.2. AI offers significant opportunities for the insurance sector such as faster and automated claims handling processes, the development of more accurate and granular risk assessments, or help

[2] Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p. 48).

[3] Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (OJ L 26, 2.2.2016, p. 19).

[4] Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (OJ L 335, 17.12.2009, p. 1).

[5] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1–79).

[6] Commission Delegated Regulation (EU) 2015/35 of 10 October 2014 supplementing Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (OJ L 12, 17.1.2015, p. 1).

[7] Commission Delegated Regulation (EU) 2017/2358 of 21 September 2017 supplementing Directive (EU) 2016/97 of the European Parliament and of the Council with regard to product oversight and governance requirements for insurance undertakings and insurance distributors (OJ L 341, 20.12.2017, p. 1).

EIOPA | Westhafen Tower, Westhafenplatz 1 | 60327 Frankfurt | Germany
Tel: +49 69-951119-20
info@eiopa.europa.eu | https://www.eiopa.europa.eu

fight against customer fraud more efficiently. However, AI can also bring new risks or increase existing ones, in particular due to the limited explainability of some AI systems, which among other things can increase the risk of bias and discriminatory outputs.

2.3. In July 2024 the Regulation (EU) 2024/1689 (the AI Act)[8] was published in the Official Journal of the European Union. The AI Act applies to all sectors of the economy and aims at ensuring a high level of protection for fundamental rights, health, and safety. The AI Act follows a risk-based approach, classifying AI systems according to different risk levels.

2.4. Among other high-risk AI systems which may be used by undertakings, the 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. Providers and users of high-risk AI systems will need to comply with a comprehensive set of governance and risk management requirements foreseen in the AI Act. Limited derogations are introduced to address overlaps with existing sectorial insurance legislation.

2.5. The remaining AI systems in insurance that are not prohibited AI practices and that are not considered to be high-risk, without prejudice of Articles 6(3), 6(4) and 7 of the AI Act, continue to operate subject to existing sectorial legislation without new requirements, with the exception of some transparency requirements (e.g. need to inform the customer that he is interacting with an AI system), the need to promote staff AI literacy, and the development of voluntary codes of conduct.

2.6. The objective of this Opinion is to provide further clarity on the main principles and requirements foreseen in insurance sectoral legislation that should be considered in relation to those insurance AI systems that are not considered as prohibited AI practices or high-risk under the AI Act; although insurance legislation such as the Insurance Distribution Directive and the Solvency II Directive, on which this Opinion is based, applies to all AI systems used in insurance, to avoid regulatory complexities and overlaps the scope of this Opinion does not cover prohibited AI practices or high-risk AI systems under the AI Act.

2.7. The Opinion 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.[9] This Opinion does not set out new requirements and in particular it does not seek to extend the requirements of the AI

[8] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024.

[9] In addition to the AI Act, the expectations set out in this Opinion are aligned with the work of other international standard setting bodies such as the Organisation for Economic Co-operation and Development (OECD) (link), the G20 (link), or the International Association of Insurance Supervisors (IAIS) (link). The Opinion also leverages on the AI governance principles report developed by EIOPA's stakeholder group on digital ethics in insurance in 2021 (link).

EIOPA | Westhafen Tower, Westhafenplatz 1 | 60327 Frankfurt | Germany
Tel: +49 69-951119-20
info@eiopa.europa.eu | https://www.eiopa.europa.eu

Act to all AI use cases in insurance, but rather it provides guidance on how different provisions of insurance sectorial legislation[10] 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. 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.

2.8. To ensure consistency at European level, this Opinion is based on the definition of AI systems adopted in the AI Act.[11] The European Commission's AI Office is mandated to provide further guidance on the definition of AI systems.[12] EIOPA is engaging with the AI Office and other relevant stakeholders to provide a sectorial perspective. Nevertheless, it is important to highlight that existing insurance 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.

Questions to stakeholders:

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

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

3. AI GOVERNANCE AND RISK MANAGEMENT FRAMEWORK

RISK-BASED APPROACH AND PROPORTIONALITY

3.1. According to Article 41 of the Solvency II Directive, insurance undertakings need to have in place an effective system of governance which provides for a sound and prudent management of the business, which shall be proportionate to the nature, scale, and complexity of the operations of the insurance or reinsurance undertaking. In a similar line, Article 25 of the Insurance Distribution Directive (IDD) requires undertakings to maintain, operate and review a process for the approval insurance products which shall be proportionate and appropriate to the nature of the insurance product. Furthermore, Articles 5 and 6 of the Digital Operational Resilience Act (DORA) require financial entities to have in place an internal ICT governance and risk management frameworks, in accordance with the principle of proportionality as set out in Article 4 of the DORA.

[10] This 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 should be noted that other legislations such as Regulation (EU) 2016/679 (General Data Protection Regulation; GDPR) may also include provisions relevant to the AI systems.

[11] Article 3 (1) of the AI Act defines AI systems as "a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments".

[12] See Article 96 (1) (f) of the AI Act

EIOPA | Westhafen Tower, Westhafenplatz 1 | 60327 Frankfurt | Germany
Tel: +49 69-951119-20
info@eiopa.europa.eu | https://www.eiopa.europa.eu

3.2. As a first step, for those AI systems that are within the scope of this Opinion, undertakings should assess the risk of the different use cases; it is acknowledged that there are varying levels of risks amongst those AI use cases that are not prohibited or considered as high-risk under the AI Act. Therefore, undertakings should assess their risk and develop governance and risk management measures adequate and proportionate to the characteristics and risks of the use cases at hand.

3.3. The impact assessment should take into account criteria such as the processing of data on a large scale, the sensitivity of the data, the extent to which the AI system can act autonomously, or the potential adverse impact that an AI system could have on the right to non-discrimination (Annex I provides additional examples of indicators that could be used to assess the impact of AI use cases).

3.4. Insurance-specific criteria should also be taken 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 customers or if it is compulsory by law. Undertakings should also assess prudential considerations such as the extent to which an AI system is used in critical activities that can impact the business continuity of an insurance undertaking. The extent to which an AI system can have an impact on the financial position of an undertaking (e.g. substantial number of claims, contracts, Gross Written Premiums, solvency ratios etc.), or on the legal obligations of an undertaking is also relevant. Reputational risks that could potentially arise from the use of AI systems in certain use cases should also be considered.

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 at hand to achieve the desired outcome i.e. the proportionality principle is applicable to all the governance and risk management measures described in this Opinion.

3.6. For example, AI systems that have a low or very limited impact on customers or on the financial commitments of undertakings would require lower data governance, human oversight or explainability measures compared to those AI systems that pose higher risks, and vice versa. 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 measures such as data governance or human oversight may be developed to compensate their lack of explainability.

Questions to stakeholders:

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

EIOPA | Westhafen Tower, Westhafenplatz 1 | 60327 Frankfurt | Germany
Tel: +49 69-951119-20
info@eiopa.europa.eu | https://www.eiopa.europa.eu

RISK MANAGEMENT SYSTEM

3.7. In line with Article 41 of the Solvency II Directive, Article 25 of the IDD, Articles 4, 5, and 6 of the DORA, in order to ensure a responsible use of AI systems that maximises the benefits of AI systems and minimises the risks, undertakings should develop proportionate governance and risk management systems, considering the following areas:

- Fairness and ethics
- Data governance
- Documentation and record keeping
- Transparency and explainability
- Human oversight
- Accuracy, robustness and cybersecurity

3.8. The responsible use of AI systems is not achieved by a standalone measure, but by a combination of different risk management measures. Therefore, the above-mentioned areas are complementary to one another and cross-references and dependencies between them are inevitable (as reflected also in this Opinion).

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 management 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 organisation changes.

3.10. 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, where the roles and responsibilities of different staff are clearly defined (see also Human oversight section below). 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.

Questions to stakeholders:

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?

FAIRNESS AND ETHICS

3.11. Article 17 of the IDD stipulates that insurance distributors shall always act honestly, fairly and professionally in accordance with the best interests of their customers. Moreover, EIOPA's 2023

EIOPA | Westhafen Tower, Westhafenplatz 1 | 60327 Frankfurt | Germany
Tel: +49 69-951119-20
info@eiopa.europa.eu | https://www.eiopa.europa.eu

Supervisory Statement on Differential Pricing Practices[13] outlines certain pricing practices that are not considered compliant with the requirement to treat customers fairly and provides guidance on the governance and risk management measures that insurers need to develop to mitigate risks.

3.12. Taking into account risk-based and proportinality considerations, undertakings should adopt a customer-centric approach to the use of AI systems throughout its entire lifecycle and across the value chain to ensure that customers are treated fairly and according to their best interest. This includes developing a corporate culture that includes ethics and fairness guidance and relevant trainings.

3.13. The data used to train and test AI systems is accurate, complete, representative and free of bias, and the outputs of AI systems should be meanigfully explainable to identify and mitigate potential bias (see the data governance and explainability sections below).

3.14. 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).

3.15. Adequate redress mechanisms should also be in place to enable customers to access and seek redress when they have been negatively affected by an AI system.

Questions to stakeholders:

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?

DATA GOVERNANCE

3.16. According to Article 260(1)(a)(ii) of the Commission Delegated Regulation 2015/35, the risk management system should include policies regarding the sufficiency and quality of relevant data for underwriting and reserving processes. Article 82 of the Solvency II Directive stipulates that data shall be complete, accurate and appropriate for calculating the technical provisions. Furthermore, Article 6(1) of the Commission Delegated Regulation 2017/2358 required that manufacturers test their insurance products appropriately, including scenario analyses where relevant.

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 legislaiton.

[13] https://www.eiopa.europa.eu/system/files/2023-03/EIOPA-BoS-23-076-Supervisory-Statement-on-differential-pricing-practices_0.pdf

EIOPA | Westhafen Tower, Westhafenplatz 1 | 60327 Frankfurt | Germany
Tel: +49 69-951119-20
info@eiopa.europa.eu | https://www.eiopa.europa.eu

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.

3.19. Sound data governance should be applied throughout the AI system life cycle in data collection, data processing and post processing.

3.20. If the undertaking makes use of external data acquired from a third party, the same data quality standards should apply.

Questions to 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?

DOCUMENTATION AND RECORD KEEPING

3.21. Article 258(1)(i) of the Commission Delegated Regulation 2015/35 requires that insurance undertakings maintain adequate and orderly records of the insurance undertaking's business and internal organisation. Furthermore, Article 9 of the Commission Delegated Regulation 2017/2358 requires that relevant actions taken by undertakings in relation to their product approval process are duly documented, kept for audit purposes and made available to the competent authorities upon request.

3.22. In the context of AI systems, and taking into account risk-based and proportionality considerations, undertakings should keep appropriate records of the training and testing data and the modelling methodologies to ensure their reproducibility and traceability.

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.

Questions to stakeholders:

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

EIOPA | Westhafen Tower, Westhafenplatz 1 | 60327 Frankfurt | Germany
Tel: +49 69-951119-20
info@eiopa.europa.eu | https://www.eiopa.europa.eu

TRANSPARENCY AND EXPLAINABILITY

3.24. Pursuant to Article 20(1) of the IDD, undertakings shall provide the customer with objective information about the insurance product in a comprehensible form to allow the customer to make an informed decision. Furthermore, Article 258(h) of the Commission Delegated Regulation 2015/35 stipulates that insurance undertakings shall establish information systems which produce complete, reliable, clear, consistent, timely and relevant information concerning the business activities, the commitments assumed and the risks to which the insurance undertaking is exposed. Moreover, according to Article 8 of the Commission Delegated Regulation 2017/2358 manufacturers shall carefully select distribution channels that are appropriate for the target market, thereby taking into account the particular characteristics of the relevant insurance products.

3.25. Undertakings should adopt the necessary measures to ensure that the outcomes of AI systems 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. Supplementary explainability tools such as LIME or SHAP[14] 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.

3.26. In application of the principle of proportionality, undertakings should adapt the explanations to specific AI use cases. If the complexity of the AI system hinders the full transparency and explainability, the undertaking should put in place complementay risk management measures such as stronger guardrails and closer human oversight. Undertakings should particularly comprehensively secure and test (before release as well as on an ongoing basis) those AI use cases that could have a high impact on customers or solvency.

3.27. The explanations should also be adapted to the recipient stakeholders. For example, for competent authorities and auditors, the undertakings should be able to provide a global and comprehensive explanation about the functioning of the AI system. For customers, in addition to being informed that they are interacting with an AI system, upon the customer's request, the influence of the AI system on the decision that has a material impact on them should be clarified using simple, clear and non-technical language to allow them to make informed decisions.

Questions to stakeholders:

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?

[14] LIME (Local Interpretable Model-Agnostic Explanations) and SHAP (Shapley Additive Explanations) are two techniques used for explainability in AI. Both focus on providing local explanations, meaning they aim to explain how specific data points or regions within the input data impact the output of an AI system.

EIOPA | Westhafen Tower, Westhafenplatz 1 | 60327 Frankfurt | Germany
Tel: +49 69-951119-20
info@eiopa.europa.eu | https://www.eiopa.europa.eu

HUMAN OVERSIGHT

3.28. According to Article 46 of the Solvency II Directive, insurance undertakings shall have in place effective internal control systems at all levels of the insurance undertaking. Furthermore, Article 258(2) of the Commission Delegated Regulation 2015/35 requires the insurance undertakings to develop policies on internal control, internal audit and where relevant outsourcing. Also, Article 7 of the Commission Delegated Regulation 2017/2358 requires that manufacturers continuously monitor and review insurance products.

3.29. Undertakings should put in place effective internal control systems depending on the nature, scale and complexity of the AI systems and during their entire lifecycle. Roles and responsibilities should be defined in policy documents to ensure that relevant staff is involved in the necessary steps of the AI system life cycle, in particular:

- 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.
- The compliance and audit functions should ensure that the use of AI systems within the organisation is compliant with all applicable laws and regulations.
- The Data Protection Officer should ensure that personal data processed by AI systems is processed in compliance with the applicable data protection rules. The actuarial function is responsible for the controls on AI systems that fall under its responsibilities (e.g. for coordination of technical provisions calculation, opinion on the overall underwriting policy).
- The undertaking may decide to create other organisational arrangements, such as apointing 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.

3.30. Sufficient training should be provided to staff to ensure that the human oversight can be effective.

3.31. Human oversight by the relevant staff should contribute to the removal of possible biases in line with the policy of the undertaking. Guardrails should be put in place to ensure that the AI system functions as designed, does not violate customers' rights and is safe.

Questions to stakeholders:

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?

EIOPA | Westhafen Tower, Westhafenplatz 1 | 60327 Frankfurt | Germany
Tel: +49 69-951119-20
info@eiopa.europa.eu | https://www.eiopa.europa.eu

ACCURACY, ROBUSTNESS AND CYBERSECURITY

3.32. According to Article 46 of the Solvency II Directive, the insurance undertaking should put in place an effective internal control system. Article 258(1)(j) and (3) of the Commission Delegated Regulation 2015/35 stipulate that the security, integrity and confidentiality of the information shall be safeguarded depending on the nature of the information. Furthermore, the DORA seeks to enhance the resilience and security of the financial system, and in particular Articles 11 (4) and (6) lay down uniform requirements concerning the security of information and communication technologies (ICT) for the financial sector, including the requirement to establish, implement, maintain and test business continuity plans.

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 developed in-house or purchased from third-party service providers.

3.34. The undertaking should use metrics, including fairness metrics, to measure the performance (accuracy, recall etc.) adapted to the AI use case in question.

3.35. AI systems should be resilient against attempts by unauthorised third parties to alter their use, outputs or performance by exploiting system vulnerabilities (e.g. data poisoning or adversarial attacks). To this extent, undertakings should have adequate and up-to-date IT infrastructure as well as fall-back plans to ensure ICT business continuity.

Questions to stakeholders:

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?

4. MONITORING BY EIOPA

4.1. Two years following the publication of this Opinion, EIOPA will look into the supervisory practices of competent authorities with a view to evaluate supervisory convergence.

4.2. EIOPA will continue collaborating with competent authorities to facilitate smooth implementation of regulation applicable to the use of AI in the insurance sector and support competent authorities in their supervisory work.

EIOPA | Westhafen Tower, Westhafenplatz 1 | 60327 Frankfurt | Germany
Tel: +49 69-951119-20
info@eiopa.europa.eu | https://www.eiopa.europa.eu

4.3. Based on the proposed AI governance framework in this Opinion, EIOPA envisages to subsequently develop more detailed analysis on specific AI use cases or issues arising from the use of AI systems in insurance and provide further guidance, as relevant.

4.4. EIOPA will continue monitoring market developments via different tools in close collaboration with stakeholders.

4.5. This Opinion will be published on EIOPA's website.

Done at Frankfurt am Main, on DayMonthYear.

[signed]

For the Board of Supervisors

Petra Hielkema

Chairperson

EIOPA | Westhafen Tower, Westhafenplatz 1 | 60327 Frankfurt | Germany
Tel: +49 69-951119-20
info@eiopa.europa.eu | https://www.eiopa.europa.eu

ANNEX I – EXAMPLES OF IMPACT ASSESSMENT INDICATORS, RECORD KEEPING AND FAIRNESS METRICS

This Annex includes practical examples of impact assessment indicators, record keeping and fairness metrics which have been extracted from the AI governance principles report developed by EIOPA's stakeholder group on digital ethics in 2021.

While these examples represent the views of EIOPA's stakeholder group on digital ethics and ultimately the undertaking concerned should develop the governance and risks management framework that best adapts to the nature, scale and complexity of their business model, they have been included in this Annex to illustrate practical ways on how to implement some of the high-level principles included in this Opinion.

1. EXAMPLES OF IMPACT ASSESSMENT INDICATORS

	AI Use case Impact Assessment	
	Impact on consumers	Impact on insurance firms
Severity	Number of consumers affected	Business continuity
	Consumer interaction and interests	Financial Impact
	Types of consumers (e.g. vulnerable consumers)	Legal impact
	Human autonomy	Reputational impact
	Anti-discrimination and diversity	
	Insurance line of business relevance	
Likelihood	Evaluation or scoring, including profiling and predicting	
	Automated-decision making with legal or similar significant effect	
	Systematic monitoring	
	Model complexity/combining datasets	
	Innovative use or applying new technological or organisational solution	
	Type and amount of data used	
	Outsourcing datasets and AI applications	

Source: EIOPA Consultative Expert Group on Digital Ethics in insurance

2. EXAMPLE OF RECORD KEEPING FOR HIGH-RISK AI USE CASES

Record	Description
Reasons for using AI	Explanation of the business objective / task pursued by using AI and its consistency with corporate strategies / objectives. Explanation of how this was implemented into the AI system. This would help avoid misuse of the AI system and enable its audit and independent review.

EIOPA | Westhafen Tower, Westhafenplatz 1 | 60327 Frankfurt | Germany
Tel: +49 69-951119-20
info@eiopa.europa.eu | https://www.eiopa.europa.eu

Integration into IT infrastructure	Description of how the model is integrated in the current IT system of the organisation and document any significant changes that could eventually take place
Staff involved in the design and implementation of the AI model	Identification of all the roles and responsibilities of the staff involved in the design and implementation of the AI model as well as their training needs. This would ensure accountability of the responsible persons.
Data collection	Documentinghow the ground truth[15] was built including how consideration was given to identifying and removing potential bias in the data. This would include explaining how input data was selected, collected and labelled.
Data preparation	Records of the data used for training the AI model, i.e. the variables with their respective domain range. This would include defining the construction of training, test and prediction dataset. For built (engineered) features, records should exist on how the feature was build and the associated intention.
Data post processing	Description of processes in place to operationalize the use of data and to achieve continuous improvement (including addressing potential bias). Records should specify the timing and frequency of data improvement actions.
Technical choices / arbitration	Documenting why a specific type of AI algorithm was chosen and not others, as well as the associated libraries with exact references. The limitation / constraints of the AI model should be documented and how they are being optimised alongside their supporting rationale. Ethical, transparency and explainability trade-offs that may apply together with their rationale should also be recorded.
Code and data	Recording the code used to build any AI model which goes to production/exploitation. Exclusively for high impact applications, insurance firms should record the training data used to build the AI model and all the associated hyper parameters, including pseudo-random seeds.[16] If this requirement proved to be too burdensome, insurance firms may put in place alternative measures that ensure the auditability of the AI model and the accountability of the firm using them.

[15] Real world data used to train and test the AI system.

[16] Pseudorandom number generator is a deterministic computational process that has one or more inputs called "seeds", and it outputs a sequence of values that appears to be random according to specified statistical tests.

EIOPA | Westhafen Tower, Westhafenplatz 1 | 60327 Frankfurt | Germany
Tel: +49 69-951119-20
info@eiopa.europa.eu | https://www.eiopa.europa.eu

Model performance	Explanations should include, inter alia, how performance is measured (KPIs) and what level of performance is deemed satisfactory, including scenario analysis and timing and frequency of reviews and / or retraining of the model. Ethical, transparency and explainability trade-offs that may apply together with their rationale should also be recorded.
Model security	Description of mechanisms in place (or makeing reference to) to ensure the model is protected from outside attacks and more subtle attempts to manipulate data or algorithms themselves: how robust is the model to manipulation attacks (especially important in auto ML models)
Ethics and trustworthy assessment	Description of the AI use case impact assessment i.e. the potential impact on customers and/or insurance firms of the concrete AI use case. Explain how the governance measures put in place throughout the AI systems lifecycle address the risks included in the AI use case impact assessment and ensure ethical and trustworthy AI systems.

Source: EIOPA Consultative Expert Group on Digital Ethics in insurance

3. EXAMPLES OF FAIRNESS METRICS[17]

Fairness metric	Description
Demographic Parity	The goal of "Demographic Parity" is to assign the positive outcome at proportionally equal rates to each subgroup of a protected class where the positive outcome refers to the favourable decision.[18] For example, in the context of a recruitment scenario "Demographic Parity" could mean that male and female candidates are invited to job interviews at equal rates, proportionately to the number of applications.
Calibration	Another approach aims at equal positive and negative predictive values for all subgroups.[19] Such calibration guarantees that the predictive values across subgroups correspond to the scores which represent the probability of predicting

[17] It is not an exhaustive list, and they may vary from one AI use case to another,

[18] Dwork, C., Hardt, M., Pitassi, T., Reingold, O., Zemel, R. (2011),

[19] Crowson, C., Atkinson. E., Therneau, T., Lawson, A., Lee, D. and MacNab, Y. (2016),

EIOPA | Westhafen Tower, Westhafenplatz 1 | 60327 Frankfurt | Germany
Tel: +49 69-951119-20
info@eiopa.europa.eu | https://www.eiopa.europa.eu

	the positive or the negative outcome. For example, in a medical diagnosis scenario, a calibrated model could ensure equal levels of confidence in the predictions for patients of different gender or ethical backgrounds because the predictive values are comparable across all subgroups.
Equalized Odds	This fairness definition requires equal true positive and true negative rates for all subgroups.[20] For example, where an insurance firms uses AI systems to scan through CVs and job applications in recruitment processes, "Equalized Odds" would ensure that the chances for men and women to be invited to the job interview are equal.[21]
Equalized Opportunities	This relaxed version of "Equalized Odds" is often used in practice because it reduces the computational complexity when working with large real-world datasets. "Equalized Opportunities" only requires the error rates for the favourable outcome to be the same but allows deviations for the unfavourable outcome. For example, in online marketing when the objective is to inform men and women at equal rates about an insurance offer, "Equalized Opportunities" could ensure that relevant segments of both groups are shown the information at equal rates. The rate of exposure to people for whom the offer is actually irrelevant may differ, however.
Individual fairness	All definitions mentioned above bind on a group level, based on one or several protected attributes. A completely different approach is "Individual Fairness" which abandons the idea of group memberships and suggests instead that any similar individuals should be treated similarly. For example, all the individuals with the same risk profile should pay the same premium for the same insurance product.

Source: EIOPA Consultative Expert Group on Digital Ethics in insurance

[20] Hardt, M., Price, E. and Srebro, N. (2016).

[21] This fairness metric is already used by some companies such as Linkedin: https://engineering.linkedin.com/blog/2021/using-the-linkedin-fairness-toolkit-large-scale-ai.

EIOPA | Westhafen Tower, Westhafenplatz 1 | 60327 Frankfurt | Germany
Tel: +49 69-951119-20
info@eiopa.europa.eu | https://www.eiopa.europa.eu

ANNEX II – SUMMARY OF QUESTIONS TO STAKEHOLDERS

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

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

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

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?

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?

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?

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?

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?

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?

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?

EIOPA | Westhafen Tower, Westhafenplatz 1 | 60327 Frankfurt | Germany
Tel: +49 69-951119-20
info@eiopa.europa.eu | https://www.eiopa.europa.eu

ANNEX III - PRIVACY STATEMENT RELATED TO PUBLIC ONLINE CONSULTATIONS AND SURVEYS

Introduction

1. EIOPA, as a European Authority, is committed to protect individuals with regard to the processing of their personal data in accordance with Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (further referred as "the Regulation").

Purpose of the processing of personal data

2. Personal data is collected and processed in order to manage online public consultations EIOPA launches, and to conduct online surveys, including via online platform EUSurvey[22], and to facilitate further communication with participating stakeholders (e.g., when clarifications are needed on the information supplied or for the purposes of follow-up discussions that the participating stakeholders may agree to in the context of the consultations or surveys).
3. The legal basis for this processing operation comprises of:
   - Regulation (EU) 1094/2010, and notably Articles 8, 10, 15, 16, 16a and 29 thereof
   - EIOPA's Public Statement on Public Consultations
   - EIOPA's Handbook on Public Consultations
4. In accordance with Article 5(1)(a) of the Regulation processing is lawful as it is necessary for the performance of a task carried out in the public interest.
5. Personal data collected are processed according to the conditions set out in the above-mentioned Regulation.

[22] See dedicated EU Survey privacy statement.

EIOPA | Westhafen Tower, Westhafenplatz 1 | 60327 Frankfurt | Germany
Tel: +49 69-951119-20
info@eiopa.europa.eu | https://www.eiopa.europa.eu

6. Data will not be used for any purposes other than the performance of the activities specified above.

Controller of the personal data processing

7. The controller responsible for processing your data is EIOPA's Executive Director.
8. Address and email address of the controller:

   Westhafen Tower, Westhafenplatz 1

   60327 Frankfurt am Main

   Germany

   fausto.parente@eiopa.europa.eu

Personal data collected

9. The personal data processed might include:
   - Personal details (e.g., name, email address, phone number)
   - Employment details

To whom are your data disclosed?

10. The personal data collected are disclosed to designated EIOPA staff members.
11. Personal data are transmitted in accordance with the relevant provisions of Regulation.

How long are your data kept?

12. Personal data collected are retained by EIOPA until the finalisation of the project the public consultation or the survey relate to. Personal data collected via EUSurvey are deleted from EUSUrvey after the response period has ended.

EIOPA | Westhafen Tower, Westhafenplatz 1 | 60327 Frankfurt | Germany
Tel: +49 69-951119-20
info@eiopa.europa.eu | https://www.eiopa.europa.eu

13. Files will not be kept beyond the periods specified above unless the personal data is rendered anonymous.

Transfer of personal data to a third country or international organisation

14. No personal data will be transferred to a third country or international organisation.

Profiling

15. No profiling is performed in the context of this processing operation.

How can you have access to your data, verify their accuracy, rectify them or object to their processing?

16. In general, you have the right to access their data, obtain from the controller a copy of your personal data in order to check the accuracy of the data held, and/or to obtain rectification or update of these data (facts) if necessary.
17. You may also ask for erasure of your data if the processing thereof is unlawful, or to have your data blocked for a period enabling the data controller to verify the accuracy, including the completeness, of the data.
18. You may object to or obtain the restriction of the processing of your personal data.
19. Where processing is based solely on your consent, you have the right to withdraw your consent to the processing of your personal data at any time.
20. For the protection of the data subjects' privacy and security, every reasonable step shall be taken to ensure that their identity is verified before granting access, or rectification, or deletion.
21. In case of rejecting of access to their personal data, data subjects can file a complaint with the EDPS.

EIOPA | Westhafen Tower, Westhafenplatz 1 | 60327 Frankfurt | Germany
Tel: +49 69-951119-20
info@eiopa.europa.eu | https://www.eiopa.europa.eu

Whom can you contact if you have questions or complaints with regard to data protection?

22. Should you wish to obtain access to or receive a copy of your personal data, their rectification, or deletion or to object, please contact:

    - the Data Protection Officer at EIOPA by email (DPO@eiopa.europa.eu) or by letter:

      EIOPA Data Protection Officer (Confidential)

      Westhafen Tower, Westhafenplatz 1

      60327 Frankfurt am Main Germany

23. All questions or complaints concerning the processing of your personal data can be addressed to EIOPA's Data Protection Officer (DPO@eiopa.europa.eu).

24. Alternatively, you can also have recourse at any time to the European Data Protection Supervisor (www.edps.europa.eu).

EIOPA | Westhafen Tower, Westhafenplatz 1 | 60327 Frankfurt | Germany
Tel: +49 69-951119-20
info@eiopa.europa.eu | https://www.eiopa.europa.eu