Our approach to Responsible AI

Based on the Responsible AI Standard, version 1.0,
Approved by the Board of Directors on August 27th, 2024, and endorsed by the Executive Committee on August 20th, 2024

INTRODUCTION

Responsible use of Artificial Intelligence (AI) is of the utmost importance to Ageas. As AI systems are increasingly being embedded in insurance business processes, it is expected that AI will be a major economic driver while also creating societal challenges. Ageas applies overarching principles to ensure ethical, secure, and accountable use of AI, aligned with regulatory expectations (such as Solvency II Directive, EU AI Act and GDPR), international standards and industry best practices (such as EIOPA AI governance principles, ISO 41001, NIST AI 100-1) as well as with Ageas organisational values.

SCOPE

Ageas Responsible AI Standard applies to **ageas SA/NV and all its Subsidiaries** and to their Staff.

For the **Subsidiaries**, should compliance with Responsible AI result in non-compliance with local legislation or regulations, the latter must take precedence. The Group Standard owner must be informed and consulted immediately in such circumstances.

For the **Affiliates** it is recognised that the requirements of the local law, the local regulator and the majority shareholder's policy applies. However, Ageas will advise similar principles with reasonable effort.

AGEAS APPROACH TO RESPONSIBLE AI

FRAMEWORK

Ageas has established a Responsible AI framework supported by policies, standards, processes and procedures integrating governance, risk management, and controls to ensure AI systems are trustworthy, secure and aligned with ethical and legal expectations. This framework forms part of the broader governance and risk management structure covering, in particular, data management, information security and personal data management, supporting sustainable and responsible business practices.

PRINCIPLES

Ageas put forward six existing principles which relate to the responsible use of AI throughout the organisation and via the Responsible AI Standard provides requirements on how to implement them in practice through the AI system's lifecycle:

- AI vendor and model related:
  - **Transparency and explainability** (requiring comprehensive information and documentation on use case design, data variables and mode parameters to explain AI outputs to relevant recipient stakeholders)
  - **Fairness, equality and sustainability** (requiring fair, sustainable and non-discriminatory development and deployment of AI systems that align with Ageas' values, ethics and applicable laws and regulations, and include elimination of biases in input and output of AI models)
  - **Collaboration and ownership** (requiring stable relationships with tech partners through

clear contractual agreements)

- Governance and operating model related:
  - **Human-centric governance** (establishment of adequate level of human oversight throughout the AI system's lifecycle; e.g., human-in the-loop)
  - **Strong data protection and privacy** practices (aligned with applicable data protection laws and regulations where data privacy and security must be designed around specific AI use cases to ensure secure, accurate and purpose-oriented data use and storage, both internally and externally)
  - **Performance and resilience** (including ongoing fit-for-purpose assessment of AI use cases to track and confirm performance and security through comprehensive metrics)

Together, these principles provide a coherent framework to align AI initiatives with ethical standards, regulatory requirements, and business objectives.

AI USE CASE LIFE CYCLE MANAGEMENT

AI systems are managed throughout their lifecycle, including following phases:

- **Design** in which the purpose, context, and capabilities of the AI system must be defined while identifying and assessing risks
- **Build** in which mitigation measures (including technical safeguards, operational controls, and appropriate levels of human oversight) must be implemented. Systems are tested and validated before deployment, and incident response mechanisms are established to manage potential disruptions
- **Run** in which AI systems are continuously monitored to ensure performance, compliance, and reliability

RISK MANAGEMENT

Ageas identifies and manages AI-related risks, including bias, lack of transparency, data protection risks, and operational risks. Risk assessments and impact analyses are performed to ensure that high-risk AI use cases are appropriately controlled and mitigated and unacceptable risk are avoided.

AWARENESS & TRAINING

Ageas invests in awareness and training to ensure that staff involved in AI understand their responsibilities and the risks associated with AI systems. Training supports compliance with the Responsible AI framework and promotes ethical use of AI.

GOVERNANCE

Roles and responsibilities regarding responsible AI are clearly defined across the organisation which allows to put defined responsible AI principles in practice.

This includes Board of Directors and Executive Committee responsibilities:

The **Board of Directors** of Ageas is ultimately accountable for the responsible use of AI in the organisation and must have sufficient understanding about how AI is used within businesses and about its potential risks.

The **Executive Committee** is responsible for integrating AI into the organisation's strategy, ensuring adequate risk treatment, resources availability, and promoting awareness and training and making sure this

is done in accordance with Ageas Responsible AI framework, applicable laws and regulations.

Business data owners, operational roles, support and control functions, each contribute to managing specific aspects of AI-related risks, including data quality, privacy, security, and regulatory compliance.

This structured model ensures that responsibility for AI is distributed across the organisation and embedded in existing governance processes.