

# Policy Statement on Responsible AI of Ping An Group

September, 2026

## **| Purpose**

To regulate the responsible artificial intelligence (AI) governance of Ping An Insurance (Group) Company of China, Ltd. (hereinafter referred to as "Ping An" or the "Ping An Group"), to ensure the safety, controllability, and reliability of AI technology applications, to promote technology-enabled compliance that empowers core business development, and to contribute to sustainable social and ecological development, Ping An hereby formulates this Policy Statement.

## **| Responsible AI Governance Principles and Measures**

Ping An adheres to the five ethical principles of "human-centricity, human autonomy, safety and controllability, fairness and impartiality, and openness and transparency." We continuously improve our responsible AI governance system, and have incorporated "AI Safety and Governance" as a core module in the Group's AI training system to reinforce compliance awareness across all employees, ensuring secure, controllable, and ethical AI technology applications.

### **Human-Centricity**

- We follow human values and ethics, promote human-machine harmony, and serve the progress of human civilization. We take social security and respect for human rights as prerequisites, avoid misuse, and prohibit abuse and malicious use.

### **Human Autonomy**

- In the application process, we ensure the right to informed consent by disclosing possible risks and impacts, and enable human intervention or oversight over every decision made by AI.
- We clearly designate business owners and technical owners for AI applications, reasonably allocate responsibilities and duties among parties, and shall not transfer responsibilities that should be borne by humans to AI applications.
- We strictly enforce the submission, approval, and supervisory control of high-risk AI applications, ensuring that critical decisions always remain under effective human control and organizational accountability mechanisms.

## Safety and Controllability

- We incorporate AI risks into our comprehensive risk management system, conduct regular assessments and reviews of AI application risks and control measures, and establish robust risk management capabilities throughout the entire AI lifecycle.
- When personal information is involved, we set boundaries at each stage—collection, storage, and use—establish institutional norms, implement security control technologies, and respect and protect personal privacy.
- We strictly enforce review processes for sensitive permission applications, granting relevant access only when authorized requirements and control policies are met.
- We implement reasonable identification, prompt, restriction, or interception of illegal, harmful, fraudulent, infringing, discriminatory, or other inappropriate content, and regularly evaluate the accuracy and effectiveness of such control measures.
- We ensure the implementation of data security governance models, enhancing data security control technologies across business systems, host security, and cybersecurity protection.

## Fairness and Impartiality

- We promote coordinated development, drive transformation and upgrading across industries, and leverage AI to empower a broad ecosystem of sectors.
- We conduct fair competition in accordance with the law, prevent improper exclusion or restriction of competition through data, algorithm, or platform advantages, and promote industry collaboration and technology universal access on a secure and compliant basis.
- Through continuous improvement in technical capabilities and management practices, we eliminate bias and discrimination at all stages—data acquisition, algorithm design, technology development, product R&D, and application deployment.

## Openness and Transparency

- We clearly label AI-generated content and outcomes, and explicitly indicate automated decision-making components.
- We establish comprehensive customer objection response mechanisms for automated decisions, provide clear and accessible channels for appeals, and continuously monitor the operation of decision-making applications to optimize the reasonable baseline of AI decisions.

- Without harming personal privacy, trade secrets, intellectual property, or system security, we disclose information on AI systems' data source categories, primary capabilities, applicable boundaries, known limitations, and governance measures, in accordance with risk levels.
- We ensure that high-risk AI applications are traceable, verifiable, and subject to internal audits, independent validation, and regulatory inspections within authorized scopes.
- We continuously monitor model performance, data drift, fairness, security, and business applicability; when significant changes or shifts in risk levels occur, we re-initiate assessment and approval processes.

## Responsible AI Governance Objectives

Ping An has established responsible AI governance objectives across four dimensions: data usage, algorithm research, industry application, and low-carbon operations.

### Data Usage

- **Full Protection of Privacy Data:** We adhere to the principles of minimum necessity and informed consent, ensuring that personal information processing does not exceed the scope authorized at the time of collection. We strictly control usage scenarios and comply with the Group's data compliance and information security requirements.
- **Prudent Handling of Sensitive Personal Information:** We ensure that the collection and processing of sensitive personal information are subject to explicit consent from the data subject, and apply encryption storage or stricter access controls and other security protection measures.

### Algorithm Research

- **Technical Transparency:** We establish model documentation systems commensurate with risk levels, ensuring that the purpose, data, limitations, and operational logic of AI applications are auditable by internal audit and regulatory authorities.
- **Algorithm Reliability:** Under intended uses and reasonably foreseeable conditions, we test model accuracy, stability, and robustness. We place special emphasis on preventing emerging AI security risks such as model hallucination, prompt injection, data poisoning, adversarial attacks, and deepfakes.

- **Decision Explainability:** For AI applications that materially affect customers' major rights and interests, we provide decision explanations appropriate to the business context, ensuring that important automated decision outcomes are traceable.
- **Result Verifiability:** We ensure that the results of algorithm operations can be reproduced under specified conditions.

## Industry Application

- **Serving Humanity:** The purpose of applying AI technology shall not contravene the fundamental direction of human ethics and morality, and shall not cause harm in its use.
- **Fairness and Non-Discrimination:** We train models using complete and relatively neutral and objective data, incorporate fairness and bias-related requirements into model capability testing systems, and strive to ensure that AI algorithms and applications are free from prejudice or discrimination.

## Low-Carbon Operations

We integrate low-ecological-footprint management into the entire lifecycle of AI-related infrastructure, adopting green and low-carbon measures during construction and maintenance to reduce environmental impact.

---

This policy is interpreted and revised by Ping An Group, and will be updated in due course according to national policies, regulatory requirements, and industry development.