Statement on Responsible and Ethical Use of Artificial Intelligence

For the purposes of this Statement Alpha Bank S.A. (the "Bank") and its relevant Group companies are collectively referred to as the "Group". References to a "Group entity" mean the Bank or the relevant Group company, as applicable.

The Group recognises the transformative potential of Artificial Intelligence ("AI") to enhance customer experience, operational efficiency, risk management and innovation. At the same time, the Group is committed to ensuring that AI is used in a lawful, ethical, secure, transparent and human-centric manner, in line with applicable legal and regulatory requirements. These may include, where applicable, Regulation (EU) 2024/1689 on Artificial Intelligence ("AI Act"), applicable national laws relating to artificial intelligence (such as Law 5321/2026), the General Data Protection Regulation ("GDPR") and the Digital Operational Resilience Act ("DORA").

The Bank's AI Policy has been approved by the Board of Directors, provides the Group framework for AI governance and applies across Alpha Bank and its Group companies subject to legal, regulatory and corporate governance requirements applicable to each entity, covering AI systems developed internally as well as AI systems provided by third parties. The Policy defines the Group's governance framework, core principles, risk-based approach and lifecycle controls for the responsible development, procurement, deployment and use of AI.

Our responsible AI principles

The Group's approach to AI is guided by the following principles:

- **Human oversight and accountability:** AI systems are subject to appropriate human oversight, as required under applicable law, particularly where they may affect customers, employees, financial decisions or regulatory compliance. Responsibilities are allocated to designated functions, without prejudice to the relevant Group entity's legal accountability.
- **Transparency and explainability:** AI systems are subject to the relevant transparency, traceability and documentation requirements, including where applicable, appropriate information on their intended purpose, functionality and limitations
- **Fairness and non-discrimination:** AI must be developed and used in ways to identify, prevent and mitigate unfair bias and unlawful discriminatory outcomes.
- **Data governance and privacy:** AI systems must respect data protection principles, including lawful processing, purpose limitation, data minimisation, data quality and appropriate safeguards for personal data.
- **Robustness, cybersecurity and resilience:** AI systems must be technically robust, secure and resilient against errors, misuse, system failures and cyber threats.
- **Responsible and sustainable use:** AI should be used in a way that supports individual, societal and environmental well-being, with consideration of longer-term social and environmental impacts.

- **Documentation and auditability:** AI development, deployment and use must be documented and auditable, supporting traceability, accountability and effective control throughout the AI lifecycle.
- **AI literacy:** Each Group entity takes appropriate measures, as required by law, to support AI literacy and role-based awareness for its staff and other persons dealing with the operation and use of AI systems on its behalf taking into account without limitation their role, level of knowledge and experience, and the nature and risks of the AI systems concerned.

Risk-based governance and boundaries of use

The Group applies a risk-based approach to AI governance. AI systems are classified according to their risk profile, taking into account the different regulatory regimes and levels of risk addressed in the AI Act, including unacceptable risk/prohibited AI practices, high-risk AI systems, limited risk / AI systems subject to specific transparency obligations and minimal risk AI systems as well as the specific framework applicable to general purpose AI models. Each AI system is documented with a clearly defined intended purpose, which forms the basis for classification, risk assessment and control requirements.

The Group prohibits the development, acquisition and use of AI systems that constitute prohibited AI practices under applicable law and maintains governance controls designed to prevent their deployment. This includes indicatively AI systems designed to manipulate behaviour in a harmful manner, exploit vulnerabilities, perform social scoring, or carry out prohibited biometric practices such as unauthorised biometric surveillance or biometric categorisation based on sensitive attributes.

Before acquisition or deployment, new AI systems are subject to appropriate review to identify their risk classification, intended use, limitations and applicable controls. High-risk AI systems are subject in accordance with the applicable statutory timelines to enhanced requirements applicable to the relevant Group entity's role, including indicatively risk assessment-management, data governance, technical documentation, record-keeping, human oversight, transparency, cybersecurity, post-deployment monitoring and, where required, Fundamental Rights Impact Assessment.

Responsible AI programmes and controls

The Group maintains programmes and controls to support the responsible use of AI throughout its lifecycle. These include an AI strategy and implementation roadmap, an AI systems register, risk classification and assessment processes, role-based training and awareness, independent validation of High-Risk AI models or models included in High-Risk systems, incident reporting and communication procedures, and oversight of third-party AI arrangements.

The Bank's governance framework assigns clear responsibilities to the Board of Directors, Executive Committee, Data and AI Governance Committee, risk and compliance functions, Group Data and AI, Data Protection Officer, cybersecurity and information security functions, business owners, model validation functions, legal, procurement and third-party risk management and HR

teams. At Group level, corresponding responsibilities are allocated as applicable to the relevant governing bodies, committees, control and business functions of each Group company. This structure supports clear accountability for the outcomes, risks and controls of AI systems.

Where a Group entity relies on third-party AI systems or services, it applies due diligence, contractual safeguards and ongoing oversight proportionate to the nature and risk of the arrangement. Such assessment may include as applicable relevant provider documentation, transparency information, declared limitations, compliance with applicable requirements and third-party risk considerations, including concentration risk where relevant.

Transparency towards customers, employees and stakeholders

Each Group entity is committed to complying with the transparency requirements applicable to the relevant AI systems. For limited-risk AI systems, such as chatbots or AI-generated content, the relevant Group entity applies transparency obligations so that users are appropriately informed when they are interacting with AI or when content has been generated by AI, where required by applicable law.

Each Group entity also applies appropriate human oversight, in accordance with applicable law, including, where relevant, the requirements for high-risk AI systems under the AI Act and the safeguards provided for under Article 22 GDPR.

Continuous improvement

The Group reviews and updates its AI Policy and related governance framework to reflect changes in applicable legal framework, regulatory developments, supervisory expectations, technological evolution and lessons learned from implementation. The Group aims to maintain effective oversight and responsible innovation while protecting the rights and interests of customers, employees and other stakeholders.