Artificial Intelligence (AI) Policy

1. Table of contents

2. Definitions

Terms not defined and written with a capital letter in this Policy have the meaning given to them in the AI Act.

2.1. AI Act - REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of June 13, 2024, on the establishment of harmonized 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)

2.2. AI system - Software or a machine that exhibits human-like intellectual capabilities such as learning, problem solving, and decision making.

2.3. AI model - An algorithm or set of algorithms that have been trained on data and are capable of performing specific tasks (e.g., classification, prediction, content generation).

2.4. AI Risk - Potential negative consequences associated with the design, development, deployment, and use of AI Systems and AI Models.

2.5. High-risk AI System - An AI System that, under the AI Act, has been identified as posing a significant risk to the health, safety, or fundamental rights of individuals and is therefore subject to strict compliance requirements and oversight.

2.6. Allegro Group/Allegro Group - Allegro.eu S.A. with its registered office in Luxembourg and any entity directly or indirectly dependent on it

2.7. Company - A company that is part of the Group

2.8. Allegro.eu S.A. Security Policy - a governing strategic document defining the organizational and technical framework for ensuring the confidentiality, integrity, and availability of information. This document forms the basis of the Information Security Management System (ISMS) and is binding on all employees.

3. Purpose

This Policy sets out the Allegro Group's commitment to the responsible development, implementation, and use of AI Systems and AI Models to ensure respect for ethical principles, appropriate risk management, and compliance with legal regulations. The main objective of this Policy is to ensure the safe and responsible use of AI Systems and AI Models within the Allegro Group.

4. Assumptions

The Policy applies to all employees and other persons who have access to AI Systems and AI Models developed and operated by Allegro.eu SA and its subsidiaries.

5. Roles, responsibilities, and oversight

5.1. The Group identifies, assesses, and minimizes risks related to artificial intelligence.

5.2. The Group defines the roles and responsibilities of individuals and teams for areas related to artificial intelligence as part of its internal procedures.

5.3. The management boards of the companies are responsible for providing the resources and support necessary to implement and comply with this Policy.

5.4. For each AI System, the Group appoints a business owner - a person responsible for its safe implementation and use within the Group.

5.5. The IT Compliance (AI Governance) team is responsible for inventorying and classifying systems, supervising data quality and periodic reviews, and testing models for bias and resilience. The team monitors key performance indicators (KPIs) and manages the process of decommissioning systems.

5.6. The Cybersecurity Offensive team is responsible for conducting vulnerability tests of AI solutions and ensuring the technical protection, confidentiality, and integrity of data used in machine learning processes.

5.7. The Data Protection team is responsible for assessing the risk and impact of systems on fundamental rights (DPIA/FRIA), registering high-risk systems, and overseeing compliance with the AI Act. The team is responsible for relations and correspondence with regulatory authorities.

5.8. The Information Security Team is responsible for defining AI standards and policies, verifying the security of third-party suppliers, managing incidents, and conducting mandatory training on ethics and the safe use of AI.

6. Principles for the safe use of AI

The Group manages the use of artificial intelligence in a continuous and responsible manner, integrating risk assessment processes and rigorous data management standards with requirements for transparency, ethics, and continuous monitoring. These activities are complemented by the systematic improvement of employee competencies through annual training cycles, which ensures security and full operational compliance with applicable regulations. In order to implement the above objectives, the Group carries out the following activities:

6.1. AI risk management

6.1.1. The Group manages the risks associated with the use of artificial intelligence on an ongoing basis, in accordance with the risk management process adopted by the Group and the adopted Risk Policy.

6.1.2. Prior to the implementation of AI Systems and AI Models, the Group conducts a risk assessment that includes the obligation to classify the AI system to the appropriate risk level and to verify that it does not constitute a prohibited system within the meaning of the AI Act. While using AI Systems and AI Models, the Group monitors the risk and, if necessary, reassesses the risk.

6.2. Data Management (Including Personal Data) in AI Systems and AI Models

The Group manages data in AI Models and AI Systems in accordance with its policy, which includes the following principles:

6.2.1. The data used in AI Systems and AI Models is adequate for the purpose, reliable, and compliant with applicable laws and internal regulations.

6.2.2. The data is complete, accurate, and up-to-date. This applies in particular to data used for training, testing, and validating AI Models.

6.2.3. Data sources are identifiable and data is subject to verification in order to reduce errors, distortions, and biases.

6.2.4. The data is adequately protected, and any significant limitations on its quality are documented and taken into account when interpreting AI results.

6.3. Transparency and explainability

6.3.1. The Group uses only AI Systems and AI Models that have adequate documentation describing, among other things, their operation, the data used, and potential limitations, in accordance with the procedures adopted by the Group and in accordance with legal requirements.

6.3.2. The Group takes measures to ensure the explainability of decisions made by AI Systems, in particular those that have a significant impact on individuals.

6.4. Ethics and bias

6.4.1. The Group takes steps to identify and minimize bias, particularly in training data and AI Models. The Group treats the avoidance of bias as a universal principle to be followed in every context of artificial intelligence, and this plays a particularly important role in high-risk AI Systems.

6.4.2. The Group implements AI Models and AI Systems responsibly, taking into account the potential impact on society and individuals.

6.5. Monitoring and audit

6.5.1. The Group monitors AI Systems, including external high-risk AI Systems, for performance, security (including cybersecurity), and compliance with the law and this Policy.

6.5.2. The Group periodically verifies the security and compliance of the use of AI Systems as part of the Group's appropriate control mechanisms.

6.6. Training and awareness

6.6.1. The Group trains employees at least once a year on the safe and ethical use of artificial intelligence.

6.6.2. The Group conducts regular awareness campaigns to raise employee awareness of the potential risks and best practices associated with artificial intelligence.

7. Responsibility for violations of the Policy

7.1. Every employee of the Group is required to comply with the provisions of this Policy.

7.2. Actions that violate the provisions of the Policy are considered prohibited, and if they occur, the Group will immediately take appropriate disciplinary and legal measures. If an employee discovers or becomes aware of a violation of this Policy, they are required to immediately report this fact to the CSO in accordance with the Whistleblowing Policy.

8. Final provisions

8.1. The Allegro Group reviews the Policy whenever there is a change in legal and factual circumstances, but at least once a year.

8.2. New employees or persons cooperating with the Allegro Group on any other legal basis are required to familiarize themselves with the rules set forth in this Policy.

Additional information:	
Approved by:	Board of Directors Allegro.eu
Owner:	CSO
Date created	January 27, 2026
Date of last review:	March 11, 2026
Current version:	1.0
Previous version:	n/a