CPRAM	**Artificial Intelligence Policy**	update : November 2026
Compliance Department		

This document aims to present the Amundi Group's approach to identifying, preventing, and managing Artificial Intelligent that may arise during the course of its activities.

CPRAM is fully integrated into the Amundi Group framework described in the policy below.

Amundi
Investment Solutions

Trust must be earned

Artificial Intelligence Policy

JULY 2025

• Document for Professional Investors only

Contents

1. **Introduction** 3
   - 1.1. Objective 3
   - 1.2. Framework for this Policy 3
   - 1.3. Definition: what is an “AI system”? 3
   - 1.4. Guiding Principles 3
   - 1.5. Roles Defined in the AI Act 4
2. **AI Governance** 5
3. **Classification of Risk Levels** 5
   - 3.1 Classification of AI Systems, criteria and regulatory obligations 5
   - 3.2 Amundi AI Systems deployment 6
4. **Use of AI Systems by Amundi employees** 6
5. **Assessment of new AI Systems or Uses** 7
6. **Implementation and Training** 8
7. **Policy Review** 8

1. Introduction

1.1. Objective

This Artificial Intelligence (AI) Policy outlines the principles and guidelines that the Amundi Group commits to follow the development, procurement, use, and management of "AI systems". It aims to ensure compliance with the European Union AI Act (Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence), Amundi "raison d'être" (Work every day in the interest of our clients and Society) and values (courage, team spirit, entrepreneurship, solidarity), ethical requirements, transparency, best interests of clients, and personal data protection. This Policy is applicable to all Amundi Group entities.

1.2. Framework for this Policy

This Policy is inspired by the principles stated by the Crédit Agricole group (the "**Group Principles**"). This Policy sets out information on how Amundi applies the CA Group Principles, and certain matters particular to Amundi in how Amundi complies with the EU AI Act.

This Policy is also part of the framework of other applicable Amundi policies, particularly in the areas of:

- data protection (including the procedure "Gouvernance de la Protection de Données Personnelles");
- information security systems and acceptable usage of information technology systems (including the document "Information Technology Internal Policy");
- Ethics Charter, common to all entities of Crédit Agricole Group, including Amundi, summarizing the principles of actions and behaviours to be observed with regards to clients and end-users.
- Amundi's Code of Conduct (https://about.amundi.com/files/nuxeo/dl/7a3fe6ad-1e3a-47dc-b2f5-26e7e4e9fdc1)

Other legislative and regulatory obligations and guidance form part of the Amundi compliance framework.

1.3. Definition: what is an "AI system"?

The EU AI Act defines an "AI system" as follows:
"a machine-based system that is 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".

As can be seen, there are a number of aspects which must be considered when analysing if a system comes within the meaning of an "AI system" and the corresponding regulation which applies to AI systems under the EU AI Act - including consideration of levels of autonomy, adaptiveness, ability to infer, and generation of outputs.

Other important concepts, definitions, and types of AI are also described in the EU AI Act and Group Principles, and different rules may apply in certain circumstances (for example in relation to a "general purpose AI model", or a "chatbot"), and so analysis on a case-by-case basis is important.

1.4. Guiding Principles

Respect for ethics and values: Amundi values will be respected, as well as ethical principles (such as those set out in the "Ethics Guidelines for Trustworthy AI")[1] . Our duties to our company, clients, investors, and our colleagues must be respected.

Regulatory Compliance: Amundi shall also comply with applicable legislation, regulation and policies.

[1] Prepared by the independent EU Commission expert group.

Risk Assessment: before deploying any AI system, a risk assessment will be conducted to identify the risks and Amundi shall make its best efforts to mitigate those risks (including matters such as operational and security risks, and risks to individual rights and society). Risk categories are described in section 3.

Bias and Fairness: our objective is to minimize biases as much as possible in the construction of our AI system algorithms in order to provide outcomes that are as fair as possible for all users, and in the best interest of our clients.

Transparency: Amundi shall provide appropriate information to the users in accordance with the EU AI Act and Group Principles. Basically, the higher the risk associated with the IA system, the more detailed information.

Data Protection and Users' rights: all personal data that may be input in an AI system will be treated in compliance with the General Data Protection Regulation and/or any other applicable Laws and Regulations. Users will be able to exercise their rights regarding data protection.

AI solutions should be human-centric: as AI systems are used to amplify human capabilities, the protection of the interests of human beings, including their well-being and safety, should be prioritized in the design, development and deployment of AI.

1.5. Roles Defined in the AI Act

The AI Act defines several key roles that are essential for the governance and compliance of AI systems:

Provider:
A provider is defined as a natural or legal person, public authority, agency, or other body that develops an AI system or a general-purpose AI model, or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.

Deployer:
A deployer is defined as a natural or legal person, public authority, agency, or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity, considering that at Amundi, the use of AI is only on professional purposes.
Deployers are responsible for ensuring that the AI system is used in compliance with applicable regulations and guiding principles in the section 1.4. They must also conduct risk assessments and ensure that the deployment of the AI system does not lead to harm or violation of rights.

User:
Individuals or entities that interact with or utilize the AI system developed or deployed by providers and deployers. Users must be informed about the capabilities and limitations of the AI system and are responsible for using it in accordance with the guidelines provided. Different considerations can apply for systems which are used by customers or which produce content for customers.

Assessment of Roles
In respect of the roles above, it is necessary that for each AI systems, an assessment takes place as to the different roles involved, who occupies each role, and what are the obligations on each party. For example, Amundi's obligations may be different depending on whether it is a Provider or a Deployer. It is also possible that roles may change as part of changing use of AI systems (for example adapting a system procured from a Provider so that the Deployer itself becomes a Provider).

2. AI Governance

Amundi has established an AI Steering Committee at Group level, which is supported at the Executive Committee level. This committee is tasked with the ethical and responsible oversight of AI development and use, ensuring that all new AI systems are aligned with Amundi's core values, policies, and compliance requirements.

The objectives of the AI Steering Committee are set out in its terms of reference, and include:

- Validate the AI roadmap, project prioritization and strategy of deployment, ensuring alignment with Amundi's Global Management Committee strategy.
- Challenge ideas presented by Amundi's business lines and determine which route the use case will follow.
- Provide "go/no go decisions" for each project.
- Review the benefits and value added for each of the solutions developed and implemented.
- Validate the proposed ongoing governance and change management of the business cases.

While the Committee has the above objectives and responsibilities, local Amundi entities may have particular local obligations under applicable legislation and regulation, and it is the responsibility of local entities to analyse if there are additional local obligations on them, or requirements for them to put in place local governance arrangements.

3. Classification of Risk Levels

3.1 Classification of AI Systems, criteria and regulatory obligations

According to the EU AI Act, AI systems are classified into different categories based on their level of risk, with specific criteria and regulatory obligations for each category:

Unacceptable Risk AI

AI systems associated with unacceptable risk usage are prohibited and cannot be implemented.

- *Criteria*: systems that pose a clear threat to safety, fundamental rights, or human dignity.
- *Obligations:* these systems are prohibited and cannot be developed, deployed, or used.
- *Examples*: Government social scoring systems, AI systems that manipulate human behaviour in harmful ways.

High Risk AI

AI systems associated with high risk are permitted by the regulatory framework but must comply with specific requirements.

- *Criteria:* systems that significantly impact individuals' rights or safety, particularly in critical areas such as AI CV classification, Algorithmic trading systems, Credit score and risk assessment, fraud detection systems, customer profiling and personalization, providing investment recommendations, or investment research to investors or clients.
- *Obligations:*
  - conduct a compliance assessment before deployment of the relevant AI system .
  - ensure high levels of data quality and management.
  - implement risk management systems.
  - maintain detailed documentation and transparency regarding the system's functioning.
  - ensure human oversight and control over the system.
  - report any serious incidents or malfunctions to the relevant authorities.
- *Examples:* system used in employment (recruitment).

Exceptions to the classification of AI systems as high-risk may exist if they do not significantly influence the outcome of the decision–making process.

Low Risk AI

The Group principles define a category of "low risk" AI systems and set out obligations in respect of such systems. These are systems which present a limited or very low risk to fundamental rights, such as AI systems used for products or services recommendations. This category includes both categories defined under the EU AI Act of "limited risk" and "minimal risk". Further information on these EU AI Act classifications is included below.

Low Risk – "Limited Risk" AI:

- *Criteria*: systems that have a moderate impact on users but do not pose significant risks to rights or safety.
- *Obligations:*
  - provide clear information to users about the use of AI, including its capabilities and limitations.
  - ensure transparency in the system's operation.
- *Examples:* internal Chatbot on procedures, AI alert tools to be used by employees, Content generated or modified with the help of AI - images, audio or video files (for example deepfakes) - need to be clearly labelled as AI generated so that users are aware when they come across such content.

Low Risk – "Minimal Risk" AI:

- *Criteria:* systems that pose negligible risk to users and do not significantly impact rights or safety.
- *Obligations:* while there are no specific regulatory requirements, best practices should be followed to ensure ethical use and data protection.
- *Examples:* AI applications used for simple tasks, such as video games or basic virtual assistants.

3.2 Amundi AI Systems deployment

Unacceptable Risk AI	**High Risk AI**	**Low Risk AI**	
		Limited Risk AI	*Minimal Risk AI*
Unacceptable AI systems are not permitted.	No high risk use cases may be implemented without the prior approval of the AI Steering Committee.	Currently *all* new AI systems require prior approval of the AI Steering Committee (even for "low risk" AI systems), however the Committee reserves the discretion to change this practice in future by way of appropriate communication.	

All proposed new AI systems must be analysed in order to classify them in accordance with the above risk classifications. More detail on required assessments is set out in section 6 below.

4. Use of AI Systems by Amundi employees

All AI systems accessible and used by Amundi employees must be pre-approved beforehand. Use of AI systems by Amundi employees is subject to restrictions. Employees are not authorized to use non approved AI systems for professional purposes.

Use of AI systems comes with risks such as loss of company data and information, risk to confidentiality and commercially sensitive information, privacy risks and risks related to protection of personal data.

Amundi employees must use AI systems in an ethical manner and not contravene company policies or protections in place in respect of these areas.
Further, AI systems may often return incorrect or incomplete results, or results which do not reflect broader consideration of overall context or background. AI systems may also have inherent risk of bias or discrimination. Employees using AI systems are educated to bear these risks in mind if using the systems. Employees should keep aware of the cybersecurity and data privacy policies and apply them when using AI systems. . To ensure confidentiality and security, non-public data should be encrypted, or risk of sensitive confidential information, such as personal data, fed into the AI system should be migrated.

More generally, the trust of clients, investors, and employees are some of Amundi's most valuable assets, and this remains a guiding principle when using AI systems.

AI systems must be used in accordance with any training or policies in place for such systems. Use of AI systems does not replace any duty of care or responsibilities which an employee has as part of his/her role in Amundi.

AI systems may only be used within the risk classification for which they have been approved – use in a higher risk context is prohibited. For example, a document analysis system which is approved for low-risk functionalities (e.g. summarizing content) must not be used for high-risk functionalities (e.g. filtering job applications and selecting which applicants to hire). Further, AI systems must never be used for "unacceptable risk" uses.

The AI systems developed and utilized by Amundi are designed to provide analyses, recommendations, and automation based on data. However, these systems do not replace human judgment and should not be used as the sole basis for making critical decisions.

5. Assessment of new AI Systems or Uses

New AI systems or new uses of AI systems are subject to an analysis and review process.

As mentioned above, Amundi will conduct an analysis of the risk classification against the classification categories set out in the EU Act, and there must also be analysis of who is performing what role according to the EU categories.

Amundi will notably make analysis of IT security, analysis of general risks, and analysis of whether the system is a special type of AI system which entails specific obligations under the EU AI Act, and determine any necessary and applicable mitigating measures in respect of risks.

The final decision on whether to approve a new AI system or new use of an AI system lies with the AI Steering Committee. In respect of local implementation or use of AI systems in particular local entities or jurisdictions, there may further be additional local governance or regulatory requirements or processes which may need to be complied with.

The EU AI Act provides that the obligations in the Act do not apply to research, testing, or development activities regarding AI systems prior to them being placed on the market or in service, however analysis of these obligations and preparation for compliance shall be done in advance of any such placement, so as to ensure compliance. A register will be maintained of the uses of AI systems by Amundi, which will contain conclusions of the assessment carried out.

6. Implementation and Training

The EU AI Act states that providers and deployers of AI systems must take measures to ensure a sufficient level of AI literacy of staff and persons dealing with the operation and use of AI systems on their behalf taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

Training: All Amundi employees involved in the development and use of AI systems will receive mandatory trainings so as to ensure compliance with EU AI Act and Group Principles, and covering topics such as ethical principles, regulatory compliance, and data protection.

7. Policy Review

This policy will be considered annually by the Amundi AI Steering Committee to ensure it remains compliant with regulatory and technological developments.

DISCLAIMER

Amundi Asset Management
Head office: 91-93, boulevard Pasteur, 75015 Paris - France.
Postal address: 91-93, boulevard Pasteur, CS 21564, 75730 Paris Cedex 15 - France.
Tel : +33 (0)1 76 33 30 30 - amundi.com
French “Société par Actions Simplifiée”- SAS with a capital stock of €1 143 615 555 - Portfolio management company approved by the French Financial Markets Authority (Autorité des Marchés Financiers) - under no.GP 04000036.
Siren no. 437 574 452 RCS Paris - Siret no. 43757445200029 - APE code: 6630 Z -
VAT identification no. FR58437574452.