CPRam	**Politique Intelligence Artificielle**	update : November 2026
Compliance Department		

Le présent document a pour objet de présenter l'approche du Groupe Amundi en matière d'identification, de prévention et de gestion des risques liés à l'intelligence artificielle susceptibles de survenir dans le cadre de ses activités.

CPR AM est pleinement intégrée au dispositif du Groupe Amundi décrit dans la politique ci-dessous.

Amundi
Investment Solutions

Trust must be earned

Politique d'intelligence artificielle

JUILLET 2025 • Document réservé aux investisseurs professionnels

Sommaire

1. Introduction 3

1.1. Objectif 3

1.2. Cadre pour cette politique 3

1.3. Définition : qu'est-ce qu'un « système d'IA » ? 3

1.4. Principes directeurs 3

1.5. Rôles définis dans la loi sur l'IA 4

2. **Gouvernance de l'IA** 5

3. **Classification des niveaux de risque** 5

3.1 Classification des systèmes d'IA, critères et obligations réglementaires 5

3.2 Déploiement des systèmes d'IA Amundi 6

4. **Utilisation des systèmes d'IA par les employés d'Amundi** 6

5. **Évaluation de nouveaux systèmes ou utilisations d'IA** 7

6. **Mise en œuvre et formation** 8

7. **Révision des politiques** 8

1. Introduction

1.1. Objectif

Cette politique d'intelligence artificielle (IA) définit les principes et directives que le groupe Amundi s'engage à suivre dans le développement, l'approvisionnement, l'utilisation et la gestion des « systèmes d'IA ». Elle vise à garantir le respect de la loi européenne sur l'IA (Règlement (UE) 2024/1689 établissant des règles harmonisées sur l' intelligence artificielle), la « raison d'être » d'Amundi (travailler chaque jour dans l'intérêt de nos clients et de la société) et des valeurs (courage, esprit d'équipe, entrepreneuriat, solidarité), exigences éthiques, transparence, intérêts supérieurs des clients et protection des données personnelles. Cette politique s'applique à toutes les entités du groupe Amidi.

1.2. Cadre de cette politique

Cette politique s'inspire des principes énoncés par le groupe Crédit Agricole (les « Principes du Groupe »). Cette politique présente des informations sur la manière dont Amundi applique les principes du groupe CA, ainsi que certains aspects propres à Amundi concernant la conformité d'Amundi à la loi européenne sur l'IA.

Cette politique fait également partie du cadre d'autres politiques applicables d'Amundi, notamment dans les domaines suivants : protection des données (y compris la procédure « Gouvernance de la Protection de Données Personnelles ») ; systèmes de sécurité de l'information et utilisation acceptable des systèmes informatiques (y compris le document « Politique interne des technologies de l'information ») ; Charte d'éthique, commune à toutes les entités du groupe Crédit Agricole, y compris Amundi, résumant les principes d'actions et de comportements à observer à l'égard des clients et des utilisateurs finaux. Code de conduite d'Amundi (https://about.amundi.com/files/nuxeo/dl/7a3fe6ad-1e3a-47dc-b2f5-26e7e4e9fdc1) D'autres obligations législatives et réglementaires ainsi que des directives font partie du cadre de conformité Amidi.

1.3. Définition : qu'est-ce qu'un « système d'IA » ?

La loi européenne sur l'IA définit un « système d'IA » comme suit :

« un système basé sur une machine conçu pour fonctionner avec des niveaux variables d'autonomie et qui peut faire preuve d'adaptabilité après déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir de l'entrée reçue, comment générer des résultats tels que des prédictions, du contenu, des recommandations ou des décisions pouvant influencer des environnements physiques ou virtuels ».

Comme on peut le constater, plusieurs aspects doivent être pris en compte lors de l'analyse pour savoir si un système relève du terme « système d'IA » et du règlement correspondant applicable aux systèmes d'IA en vertu de la loi européenne sur l'IA – y compris la prise en compte des niveaux d'autonomie, d'adaptabilité, de capacité à inférer et de génération de résultats.

D'autres concepts, définitions et types importants d'IA sont également décrits dans la loi européenne sur l'IA et les Principes de groupe, et différentes règles peuvent s'appliquer dans certaines circonstances (par exemple en ce qui concerne un « modèle d'IA à usage général » ou un « chatbot »), ce qui rend l'analyse au cas par cas importante.

1.4. Principes directeurs

Respect de l'éthique et des valeurs : Les valeurs d'Amundi seront respectées, ainsi que les principes éthiques (tels que ceux énoncés dans les « Lignes directrices éthiques pour une IA digne de confiance »). Nos devoirs envers notre entreprise, nos clients, nos investisseurs et nos collègues doivent être respectés.

Conformité réglementaire : Amundi doit également se conformer à la législation, réglementation et politiques applicables.

[1] Préparé par le groupe d'experts indépendant de la Commission européenne.

Évaluation des risques : avant de déployer tout système d'IA, une évaluation des risques sera réalisée pour identifier les risques et Amundi fera de son mieux pour atténuer ces risques (y compris des questions telles que les risques opérationnels et de sécurité, ainsi que les risques pour les droits individuels et la société). Les catégories de risques sont décrites à la section 3.

Biais et équité : notre objectif est de minimiser autant que possible les biais dans la construction de nos algorithmes de systèmes d'IA afin d'obtenir des résultats aussi équitables que possible pour tous les utilisateurs et dans l'intérêt de nos clients.

Transparence : Amundi doit fournir aux utilisateurs des informations appropriées conformément à la loi européenne sur l'IA et aux principes du groupe. En gros, plus le risque associé au système IA est élevé, plus les informations sont détaillées.

Protection des données et droits des utilisateurs : toutes les données personnelles pouvant être saisies dans un système d'IA seront traitées conformément au Règlement général sur la protection des données et/ou à toute autre législation et réglementation applicables. Les utilisateurs pourront exercer leurs droits en matière de protection des données.

Les solutions d'IA doivent être centrées sur l'humain : comme les systèmes d'IA sont utilisés pour amplifier les capacités humaines, la protection des intérêts humains, y compris leur bien-être et leur sécurité, doit être priorisée dans la conception, le développement et le déploiement de l'IA.

1.5. Rôles définis dans la loi sur l'IA

La loi sur l'IA définit plusieurs rôles clés essentiels à la gouvernance et à la conformité des systèmes d'IA :

Fournisseur :

Un fournisseur est défini comme une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe un système d'IA ou un modèle d'IA à usage général, ou qui possède un système d'IA ou un modèle d'IA à usage général développé et le met sur le marché, ou met le système d'IA en service sous son propre nom ou marque, que ce soit contre paiement ou gratuitement.

Déploieur :

Un déployeur est défini comme une personne physique ou morale, une autorité publique, une agence ou tout autre organisme utilisant un système d'IA sous son autorité, sauf lorsque le système d'IA est utilisé dans le cadre d'une activité personnelle non professionnelle, étant donné qu'à Amundi, l'utilisation de l'IA ne concerne que des fins professionnelles.

Les déployeurs sont responsables de s'assurer que le système d'IA est utilisé conformément aux réglementations et principes directeurs applicables à l'article 1.4. Ils doivent également effectuer des évaluations des risques et veiller à ce que le déploiement du système d'IA ne conduise pas à des préjudices ou à des violations de droits.

Utilisateur :

Les individus ou entités qui interagissent avec ou utilisent le système d'IA développé ou déployé par les fournisseurs et les déployeurs. Les utilisateurs doivent être informés des capacités et des limites du système d'IA et être responsables de son utilisation conformément aux directives fournies. Différentes considérations peuvent s'appliquer aux systèmes utilisés par les clients ou qui produisent du contenu pour eux.

Évaluation des rôles

En ce qui concerne les rôles mentionnés ci-dessus, il est nécessaire que pour chaque système d'IA, une évaluation soit réalisée des différents rôles impliqués, de qui occupe chaque rôle et des obligations de chaque partie. Par exemple, les obligations d'Amundi peuvent varier selon qu'il s'agit d'un Fournisseur ou d'un Déploieur. Il est également possible que les rôles évoluent dans le cadre de l'évolution de l'utilisation des systèmes d'IA (par exemple, adapter un système acquis auprès d'un Fournisseur afin que le Déploieur lui-même devienne un Fournisseur).

2. Gouvernance de l'IA

Amundi a mis en place un Comité de pilotage de l'IA au niveau du Groupe, soutenu au niveau du Comité Exécutif. Ce comité est chargé d'assurer la supervision éthique et responsable du développement et de l'utilisation de l'IA, en veillant à ce que tous les nouveaux systèmes d'IA soient alignés sur les valeurs fondamentales, les politiques et les exigences de conformité d' Amundi.

Les objectifs du Comité de pilotage de l'IA sont définis dans son mandat et comprennent : Valider la feuille de route de l'IA, la priorisation des projets et la stratégie de déploiement, afin d'assurer l'alignement avec la stratégie du Comité de gestion mondiale d'Amundi.

Remettre en question les idées présentées par les lignes métier d'Amundi et déterminer la voie que suivra le cas d'usage. Proposer des décisions « go/no go » pour chaque projet.

Examiner les avantages et la valeur ajoutée de chacune des solutions développées et mises en œuvre. Valider la gouvernance continue et la gestion du changement proposées des business cases.

Bien que le Comité ait les objectifs et responsabilités mentionnés ci-dessus, les entités locales d'Amundi peuvent avoir des obligations locales particulières en vertu de la législation et de la réglementation applicables, et il incombe aux entités locales d'analyser s'il existe des obligations locales supplémentaires ou des exigences pour mettre en place des dispositifs de gouvernance locale.

3. Classification des niveaux de risque

3.1 Classification des systèmes d'IA, critères et obligations réglementaires

Selon la loi européenne sur l'IA, les systèmes d'IA sont classés en différentes catégories en fonction de leur niveau de risque, avec des critères et des obligations réglementaires spécifiques pour chaque catégorie :

IA à risque inacceptable

Les systèmes d'IA associés à une utilisation inacceptable des risques sont interdits et ne peuvent pas être mis en œuvre.

- Critères : *systèmes qui représentent une menace claire pour la sécurité, les droits fondamentaux ou la dignité humaine.*
- Obligations : *ces systèmes sont interdits et ne peuvent pas être développés, déployés ou utilisés.*
- Exemples : *systèmes gouvernementaux de notation sociale, systèmes d'IA qui manipulent le comportement humain de manière nuisible.*

IA à haut risque

Les systèmes d'IA associés à haut risque sont autorisés par le cadre réglementaire mais doivent respecter des exigences spécifiques.

- Critères :
  - des systèmes qui impactent significativement les droits ou la sécurité des individus, en particulier dans des domaines critiques tels que la classification des CV par IA, les systèmes de trading algorithmique, l'évaluation du score de crédit et des risques, les systèmes de détection de fraude, le profilage et la personnalisation des clients, la fourniture de recommandations d'investissement, la recherche d'investissement aux investisseurs ou clients.

ou

- *Obligations :*
  - une évaluation de conformité avant le déploiement du système d'IA concerné.
  - un haut niveau de qualité et de gestion des données.
  - en place des systèmes de gestion des risques.
  - Maintenir une documentation détaillée et une transparence concernant le fonctionnement du système.
  - la supervision humaine et le contrôle du système.
  - Signaler tout incident grave ou dysfonctionnement aux autorités compétentes.
- Exemples : *système utilisé en emploi (recrutement).*

Des exceptions à la classification des systèmes d'IA comme à haut risque peuvent exister si elles n'influencent pas de manière significative le résultat du processus décisionnel. IA à faible risque Les principes du Groupe définissent une

catégorie de systèmes d'IA « à faible risque » et définissent des obligations à l'égard de ces systèmes. Ce sont des systèmes qui présentent un risque limité ou très faible pour les droits fondamentaux, comme les systèmes d'IA utilisés pour des recommandations de produits ou services. Cette catégorie inclut les deux catégories définies par la loi européenne sur l'IA de « risque limité » et « risque minimal ». Des informations complémentaires sur ces classifications de la loi européenne sur l'IA sont incluses ci-dessous.

Faible risque – IA « à risque limité » :

- Critères : *systèmes ayant un impact modéré sur les utilisateurs mais ne présentant pas de risques significatifs pour les droits ou la sécurité.*
- Obligations :
  - o des informations claires aux utilisateurs sur l'utilisation de l'IA, y compris ses capacités et ses limites.
  - o la transparence dans le fonctionnement du système.
- Exemples : *chatbot interne sur les procédures, outils d'alerte IA à utiliser par les employés, contenu généré ou modifié à l'aide de l'IA – images, fichiers audio ou vidéo (par exemple deepfakes) – doit être clairement identifié comme généré par IA afin que les utilisateurs soient informés lorsqu'ils tombent sur ce type de contenu.*

Faible risque – IA « à risque minimal » :

- Critères : *systèmes qui présentent un risque négligeable pour les utilisateurs et qui n'impactent pas significativement les droits ou la sécurité.*
- Obligations : *bien qu'il n'y ait pas d'exigences réglementaires spécifiques, les meilleures pratiques doivent être suivies pour garantir une utilisation éthique et la protection des données.*
- Exemples : *applications d'IA utilisées pour des tâches simples, comme les jeux vidéo ou les assistants virtuels basiques.*

3.2 Déploiement des systèmes d'IA Amundi

IA à risque inacceptable	**IA à haut risque**	**IA à faible risque**	
		IA à risque limité	*IA à risque minimal*
Les systèmes d'IA inacceptables ne sont pas autorisés.	Aucun cas d'utilisation à haut risque ne peut être mis en œuvre sans l'approbation préalable du Comité directeur de l'IA.	Actuellement , tous *les nouveaux systèmes d'IA nécessitent l'approbation préalable du Comité de Pilotage de l'IA* (même pour les systèmes d'IA « à faible risque »), cependant le Comité réserve la discrétion de modifier cette pratique à l'avenir par le biais d'une communication appropriée.	

Tous les nouveaux systèmes d'IA proposés doivent être analysés afin de les classer conformément aux classifications de risque ci-dessus. Plus de détails sur les évaluations requises sont exposés à la section 6 ci-dessous.

4. Utilisation des systèmes d'IA par les employés d'Amundi

Tous les systèmes d'IA accessibles et utilisés par les employés d'Amundi doivent être pré-approuvés à l'avance. L'utilisation des systèmes d'IA par les employés d'Amundi est soumise à des restrictions. Les employés ne sont pas autorisés à utiliser des systèmes d'IA non approuvés à des fins professionnelles.

L'utilisation des systèmes d'IA comporte des risques tels que la perte des données et informations de l'entreprise, le risque de confidentialité et d'informations commercialement sensibles, les risques liés à la vie privée et les risques liés à la protection des données personnelles.

Les employés d'Amundi doivent utiliser les systèmes d'IA de manière éthique et ne pas contrevenir aux politiques ou protections de l'entreprise en vigueur dans ces domaines.

De plus, les systèmes d'IA peuvent souvent fournir des résultats incorrects ou incomplets, ou des résultats qui ne reflètent pas une prise en compte plus large du contexte ou du contexte général. Les systèmes d'IA peuvent également présenter un risque inhérent de biais ou de discrimination. Les employés utilisant des systèmes d'IA sont formés à prendre ces risques à l'esprit lorsqu'ils utilisent ces systèmes. Les employés doivent rester informés des politiques de cybersécurité et de confidentialité des données et les appliquer lors de l'utilisation de systèmes d'IA. . Pour garantir la confidentialité et la sécurité, les données non publiques doivent être chiffrées, ou le risque d'informations sensibles et confidentielles, telles que les données personnelles, introduites dans le système d'IA, doit être migré.

Plus généralement, la confiance des clients, investisseurs et employés est parmi les atouts les plus précieux d'Amundi, et cela reste un principe directeur lors de l'utilisation des systèmes d'IA.

Les systèmes d'IA doivent être utilisés conformément à toute formation ou politique en place pour ces systèmes. L'utilisation des systèmes d'IA ne remplace aucun devoir de diligence ou responsabilités qu'un employé a dans le cadre de son rôle à Amundi.

Les systèmes d'IA ne peuvent être utilisés que dans la classification de risque pour laquelle ils ont été approuvés – l'utilisation dans un contexte à risque élevé est interdite. Par exemple, un système d'analyse de documents approuvé pour des fonctionnalités à faible risque (par exemple, le résumé du contenu) ne doit pas être utilisé pour des fonctionnalités à haut risque (par exemple, filtrer les candidatures et sélectionner les candidats à embaucher). De plus, les systèmes d'IA ne doivent jamais être utilisés pour des usages « à risque inacceptable ».

Les systèmes d'IA développés et utilisés par Amundi sont conçus pour fournir des analyses, des recommandations et une automatisation basée sur les données. Cependant, ces systèmes ne remplacent pas le jugement humain et ne doivent pas servir de base unique pour prendre des décisions critiques.

5. Évaluation de nouveaux systèmes ou utilisations de l'IA

Les nouveaux systèmes d'IA ou les nouvelles utilisations des systèmes d'IA font l'objet d'un processus d'analyse et d'examen.

Comme mentionné précédemment, Amundi réalisera une analyse de la classification des risques par rapport aux catégories de classification définies dans la loi de l'UE, et il doit également y avoir une analyse de qui joue quel rôle selon les catégories de l'UE.

Amundi effectuera notamment des analyses de la sécurité informatique, des risques généraux, et une analyse de la nature particulière du système d'IA impliquant des obligations spécifiques en vertu de la loi européenne sur l'IA, et déterminera les mesures d'atténuation nécessaires et applicables concernant les risques.

La décision finale d'approuver un nouveau système d'IA ou une nouvelle utilisation d'un système d'IA revient au Comité directeur de l'IA. En ce qui concerne la mise en œuvre ou l'utilisation locale des systèmes d'IA dans des entités ou juridictions locales particulières, il peut également y avoir des exigences ou processus supplémentaires de gouvernance locale ou de réglementation qui pourraient devoir être respectés.

La loi européenne sur l'IA prévoit que les obligations de la loi ne s'appliquent pas aux activités de recherche, de test ou de développement concernant les systèmes d'IA avant leur mise sur le marché ou leur mise en service, cependant l'analyse de ces obligations et la préparation à la conformité doivent être effectuées avant tout placement de ce type, afin d'en garantir la conformité. Un registre sera tenu par Amendi des utilisations des systèmes d'IA, qui contiendra les conclusions de l'évaluation effectuée.

6. Mise en œuvre et formation

La loi européenne sur l'IA stipule que les fournisseurs et déploieurs de systèmes d'IA doivent prendre des mesures pour garantir un niveau suffisant d'alphabétisation en IA du personnel et des personnes chargées de l'exploitation et de l'utilisation des systèmes d'IA en leur nom, en tenant compte de leurs connaissances techniques, de leur expérience, de leur éducation et de leur formation, du contexte dans lequel les systèmes d'IA seront utilisés, et en tenant compte des personnes ou groupes de personnes sur lesquels les systèmes d'IA doivent être utilisés.

Formation : Tous les employés d'Amundi impliqués dans le développement et l'utilisation des systèmes d'IA recevront des formations obligatoires afin de garantir le respect de la loi européenne sur l'IA et des principes de groupe, couvrant des sujets tels que les principes éthiques, la conformité réglementaire et la protection des données.

7. Revue des politiques

Cette politique sera examinée chaque année par le Comité directeur d'Amundi AI afin de garantir qu'elle reste conforme aux évolutions réglementaires et technologiques.

AVERTISSEMENT

Amundi Asset Management
Siège social : 91-93, boulevard Pasteur, 75015 Paris - France.
Adresse postale : 91-93, boulevard Pasteur, CS 21564, 75730 Paris Cedex 15 - France. Tel : +33 (0)1 76 33 30 30 - amundi.com Société par Actions Simplifiée française - SAS avec un capital social de 1 143 615 555 € - Société de gestion de portefeuille agréée par l'Autorité des Marchés Financiers (Autorité des Marchés Financiers) - sous le numéro GP 04000036.

Sirène n° 437 574 452 RCS Paris - Siret n° 43757445200029 - code APE : 6630 Z - Identification TVA n° FR58437574452.