HUB FRANCE IA

OPERATIONNALISATION DU REGLEMENT EUROPEEN SUR L'INTELLIGENCE ARTIFICIELLE (RIA)

Septembre 2026

LA POSTE

SOCIETE GENERALE

A propos du Hub France IA

Le Hub France IA est une association loi 1901 d'intérêt général dont la mission est d'accompagner l'adoption d'une IA responsable, éthique et souveraine et de soutenir son déploiement en France et en Europe. Association indépendante, son rôle est d'éclairer et influencer le débat sur les grands enjeux de l'IA.

Le Hub France IA rassemble Grands groupes, PME & ETI, startups, ESN et éditeurs, collectivités, institutions, services de l'état, écoles, fonds d'investissement, cabinets de conseils et juridiques, tous mobilisés pour produire ensemble les communs de l'IA nécessaires à son accélération.

Guidé par la rigueur scientifique et technique, le Hub France IA produit de nombreuses publications annuelles pour accompagner les entreprises, les citoyens et les pouvoirs publics vers une meilleure compréhension de l'IA, diffuser des bonnes pratiques et sensibiliser à l'impact de l'IA.

TABLE DE MATIERES

INTRODUCTION : 5

I. DATES CLÉS 8

II. DÉFINITIONS CLÉS 11

II.1 Système d'IA (SIA) 14
II.2 Risques 15
II.3 Performances d'un SIA 16
II.5 Modification substantielle 17
II.6 Données biométriques 18
II.7 Modèle *GPAI* 19
II.8 Risque systémique 21
II.9 Système d'IA a usage général 22
II.10 Finalité et destination 23
II.11 Qualification des acteurs 24

III. DÉFINITION D'UN PROJET 28

III.1 Introduction 28
III.2 Idéation 29
III.3 Priorisation et filtrage 30
III.4 Faisabilité et préanalyse des risques 31
III.5 Feuillet 33
III.6 Concept clé : fiche projet 36

IV. OBJECTIF MÉTIERS 39

IV.1 Introduction 39
IV.2 Analyse des besoins métiers 39
IV.3 Décision de lancement 40
IV.4 Spécification des objectifs métiers 40
IV.5 Feuillet 42

V. GOUVERNANCE DES DONNEES 46

V.1 Introduction 46
V.2 collecte des données 47
V.3 connaissance des données 48
V.4 Prétraitement et enrichissement des données 50

V.5 Feuillet 53
V.6 Concept clé : les données dans le RIA 56

VI. CLASSIFICATION RIA : SCENARRII DE CLASSIFICATION 58
VI.1 Introduction 58
VI.2 Feuillet 60

VII. MODELISATION 64
VII.1 Introduction 64
VII.2 Modélisation – Focus Haut Risque 65
VII.3 Modélisation – Focus modèles *GPAI* 67
VII.4 Feuillet 70
VII.5 Concept clé : Documentation technique du système d'IA 74
VII.6 Concept clé : Notice d'utilisation 76

VIII. PRODUCTION 78
VIII.1 Introduction 78
VIII.2 Déploiement du système 78
VIII.3 Surveillance du système 79
VIII.4 Maintenance du système 81
VIII.5 Feuillet 83

IX. TRANSFERT AU METIER 86
IX.1 Introduction 86
IX.2 Identifier les rôles 86
IX.3 Accompagner la transformation 86
IX.4 Évaluer les usages 88
IX.5 Feuillet 89

X. CERTIFICATION 92
X.1 Introduction 92
X.2 Feuillet 94
X.3 Bibliographie 97
X.4 ANNEXE : *CHECKLIST* POUR VOUS AIDER À OPÉRATIONNALISER LE RIA 100
X.5 Contributeurs 102

HUB FRANCE IA

Introduction

INTRODUCTION :

Le groupe de travail (GT) du Hub France IA « Boussole de l'*AI Act* » (BAIA) est né d'un constat : l'entrée en vigueur du règlement européen sur l'IA (RIA)[1] pose un nombre important de défis aux opérateurs qui interviennent dans la chaîne de production et de déploiement d'un système d'IA (SIA).

Les travaux menés ont voulu répondre à un double objectif : faciliter la mise en conformité des fournisseurs et déployeurs des SIA et poser les bases pour une acculturation à la réglementation de l'écosystème de l'intelligence artificielle (IA) en France.

Le RIA applique du langage et une logique normatifs ainsi qu'une vision « produit » à une technologie, ce qui rend ce texte complexe, tant d'un point de vue conceptuel que dans sa mise en œuvre. Cette approche nécessite de mettre en place une lecture transversale et interdisciplinaire du texte, afin de décrypter les concepts qui se cachent derrière les terminologies choisies et de faciliter, *in fine*, la vie des opérateurs de SIA.

Ceci passe tout d'abord par l'élaboration d'un langage commun partagé entre les *data scientists* et les juristes experts, rendue possible par l'écosystème composite et multidisciplinaire que fédère le Hub France IA.

Ensuite, une méthodologie de mise en conformité est proposée, avec une approche qui se veut **opérationnelle** et qui place la démarche projet au cœur du processus, de façon à garantir la conformité d'un SIA tout au long de son cycle de vie.

Concrètement, le GT BAIA a produit des fiches pratiques et infographies, qui sont consolidées dans ce livre blanc, dans lequel vous trouverez les fiches ainsi que :

- le décryptage des principales définitions du règlement ;
- des boites à outils ;
- des checklists des livrables attendus dans le cadre de la règlementation ;

[1] Parlement Européen. Conseil de l'Union européenne, Règlement (UE) 2024/1689 du Parlement Européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) no 300/2008, (UE) no 167/2013, (UE) no 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle), *2024/1689*. 12 juillet 2024. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L_202401689, (version consolidée au 27/07/2026).

- des *templates* pour préparer votre documentation.

Compte tenu du caractère récent et évolutif de la législation, ce document constitue une photographie des exigences prévues à la date de sa publication. La publication de documents tels que des lignes directrices, ou des nouvelles réglementations pourraient impacter son contenu.

HUB FRANCE IA

I. RIA - Dates clés

I. *RIA* – DATES CLÉS

Le RIA prévoit une entrée en application échelonnée dans le temps afin de répondre aux exigences opérationnelles et de laisser aux acteurs le temps de se préparer à la nouvelle réglementation.

Le **2 août 2026**[2], correspond à la date d'entrée en application de la plupart des dispositions du règlement.

L'adoption de l'Omnibus[3] a validé le décalage du calendrier initialement prévu par le RIA, en particulier en ce qui concerne l'entrée en application des dispositions relatives aux SIA à haut risque, actuellement reporté au **2 décembre 2027**.

À ce jour, le calendrier d'entrée en application est celui présenté dans l'infographie ci-dessous, qui modifie celui publié en juillet 2024.

[2] *Ibid.* (Art. 113, RIA), (voir note de bas de page **Erreur ! Signet non défini.**)
[3] Parlement Européen et Conseil de la Commission Européenne. Règlement (UE) 2026/1744 du Parlement Européen et du Conseil modifiant les règlements (UE) 2024/1689, (UE) 2018/1139 et (UE) 2023/1230 en ce qui concerne la simplification de la mise en œuvre des règles harmonisées concernant l'intelligence artificielle (train de mesures omnibus numérique sur l'IA). 8 juillet 2026. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32026R1744&qid=1786372654521

RIA – Dates clés

OBJECTIFS

- **Supprimer ou modifier ses SIA interdits**
- **Garantir un niveau suffisant de maîtrise de l'IA**
- **Mettre en conformité les nouveaux modèles *GPAI***
- **Mettre en conformité les SIA à haut risque**
- **Mettre en conformité tous les modèles *GPAI***

DATES CLES

Publication au JOUE

12 juillet 2024	2 août 2024	2 février 2025	2 mai 2025	2 août 2025	2 août 2026	2 décembre 2027	2 décembre 2028	2 août 2030
	Entrée en vigueur du RIA	Dispositions sur les **SIA Interdits** applicables	**Codes de bonnes pratiques pour les fournisseurs de modèles *GPAI***	Dispositions sur la **mise en conformité des modèles *GPAI* applicables**	Plupart de dispositions de l'**art. 50 RIA – obligations de transparence**	Dispositions sur les **SIA à haut risque (Annexe III)** applicables	Dispositions sur les **SIA à haut risque (Annexe I)** applicables et sur les **modèles *GPAI* mis sur le marché avant le 1er août 2025 (111.3)** applicables	Dispositions sur les **SIA qui sont des composants des systèmes d'information à grande échelle (Annexe X) mis sur le marché avant le 1er août 2027 (111.1)** applicables

SPECIFICITES D'APPLICATION

- **Les modèles *GPAI* mis sur le marché avant cette date bénéficient d'un délai supplémentaire de 24 mois**
- **Les SIA à haut risque mis sur le marché avant cette date sont concernés par le RIA uniquement s'ils ont subi des modifications substantielles dans la conception (111.2)**
- **Les SIA à haut risque destinés à être utilisés par les autorités publiques (111.2) doivent être mis en conformité à cette date**

RECOMMANDATIONS DU HUB FRANCE IA

- Actions de sensibilisation/formation à conduire
- Constituer un pool d'experts et mettre en place la gouvernance
- Opérationnaliser la mise en conformité
- Cartographier ses SIA
- Cartographier ses modèles *GPAI*
- Qualifier le niveau de risque des systèmes et modèles et les rôles de l'organisation
- Dresser la liste des obligations applicables
- **Documenter sa conformité**

Compléments attendus

Normes harmonisées

- Gestion des risques
- Qualité et gouvernance des données
- Journalisation (*Logging*)
- Transparence
- Supervision humaine
- Précision
- Robustesse
- Cybersécurité
- Gestion de la qualité
- Evaluation de conformité

Publication prévue à partir de début 2027

LEXIQUE

JOUE = Journal officiel de L'Union Européenne
EM = Etats membres
ANC = Autorité Nationale Compétente

HUB FRANCE IA

II. RIA - Définitions clés

II. RIA – DÉFINITIONS CLÉS

Le RIA repose sur plusieurs définitions clés, établies à l'article 3 du règlement. Dès les premières étapes du GT BAIA, l'un des enjeux majeurs a été d'identifier les notions pivots devant être parfaitement comprises avant de définir l'opérationnalisation de tout projet d'IA. À cet effet, des fiches thématiques ont été publiées entre septembre et octobre 2024.

Compte tenu des nouveaux éléments apparus depuis ces publications, il semble pertinent d'ajouter une section dédiée aux précisions apportées entre-temps par la Commission européenne. En complément de ces précisions, de nouvelles fiches thématiques relatives aux rôles définis dans le RIA ont été ajoutées. Il convient de préciser que **ces rôles ne sont pas mutuellement exclusifs** et **peuvent se cumuler**.

Voici les *addendas* relatifs aux définitions ayant fait l'objet de précisions de la part de la Commission :

- **système d'IA (SIA)** : les lignes directrices finalisées par la Commission européenne le 29 juillet 2025[4] apportent des éclaircissements sur la qualification d'un SIA. Ce document détaille les sept critères permettant de qualifier un SIA, tout en fournissant des exemples concrets et des cas d'exclusion. On notera un intérêt pratique particulier pour les précisions concernant la capacité d'inférence et, par extension, la liste des systèmes qui ne doivent pas être qualifiés de SIA (voir section 5.2 « Systèmes qui ne relèvent pas de la définition du SIA »).
- **risques** : cette fiche de synthèse présente les quatre catégories de risques définies par le RIA. Il est important de souligner que les lignes directrices clarifiant la classification des SIA comme « systèmes interdits » ont été finalisées par la Commission le 29 juillet 2025[5]. Par ailleurs, il convient de noter que ces catégories ne sont pas cloisonnées : les exigences peuvent être cumulatives. Pour offrir une vision claire de ce point complexe, un feuillet spécifique a été publié afin

[4] Commission européenne. La Commission publie des lignes directrices sur la définition des systèmes d'IA afin de faciliter l'application des règles de la première législation sur l'IA | Bâtir l'avenir numérique de l'Europe. 6 février 2025. https://digital-strategy.ec.europa.eu/fr/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application

[5] Commission européenne. La Commission publie les lignes directrices sur les pratiques interdites en matière d'intelligence artificielle (IA), telles que définies par la législation sur l'IA. | Bâtir l'avenir numérique de l'Europe. 4 février 2025. https://digital-strategy.ec.europa.eu/fr/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act

d'illustrer les différents scénarios possibles lors du déploiement d'un système (voir section « RIA : différents *scenarii* de classification »).

- Modèle d'IA à usage général (*GPAI*) : le 10 juillet 2025 a été publié le **Code de bonnes pratiques**[6], un cadre d'application volontaire visant à faciliter la mise en conformité des fournisseurs d'IA avec les obligations du RIA en matière de transparence, de droits d'auteur et de sécurité. Ce Code est assorti de **lignes directrices**[7] applicatives essentielles qui dissipent de nombreuses zones d'ombre quant à la définition des rôles des différents acteurs impliqués, aux critères de qualification d'un modèle *GPAI* et aux obligations qui s'y rattachent.

Pour établir cette classification, le document s'appuie notamment sur le considérant 98[8], qui précise qu'un modèle doté d'au moins un milliard de paramètres et entraîné sur un vaste ensemble de données présente une généralité significative, ainsi que sur le considérant 99[9], qui désigne les grands modèles d'IA génératifs comme des exemples typiques des modèles *GPAI*.

L'approche adoptée par la Commission européenne repose sur l'évaluation de la « ***puissance de calcul utilisée pour l'entraînement*** », un indicateur pertinent puisqu'il combine les deux notions complémentaires que sont le nombre de paramètres et le nombre d'exemples d'entraînement qui soit raisonnablement aisé à estimer par les fournisseurs.

Ainsi, un seuil indicatif a été fixé à 10^{23} *FLOPs* pour identifier un modèle *GPAI*, à condition que le modèle soit également capable de générer du langage, ou de produire des images ou des vidéos à partir d'un texte. Toutefois, même si un modèle remplit ces critères quantitatifs, une exception reste applicable s'il est établi qu'**il ne présente pas une généralité significative** ou qu'**il n'est pas capable d'exécuter** de manière compétente **un large éventail de tâches distinctes**.

---

[6] Commission européenne. Le code de bonnes pratiques de l'IA à usage général | Bâtir l'avenir numérique de l'Europe. 31 juillet 2026. https://digital-strategy.ec.europa.eu/fr/policies/contents-code-gpai

[7] Commission européenne. Lignes directrices à l'intention des fournisseurs de modèles d'IA à usage général | Bâtir l'avenir numérique de l'Europe. 28 avril 2026. https://digital-strategy.ec.europa.eu/fr/policies/guidelines-gpai-providers

[8] Cons. 98 : Alors que la généralité d'un modèle pourrait, entre autres, également être déterminée par un nombre de paramètres, les modèles comptant au moins un milliard de paramètres et entraînés à l'aide d'un grand nombre de données utilisant l'auto-supervision à grande échelle devraient être considérés comme présentant une généralité significative et exécutant de manière compétente un large éventail de tâches distinctes.

[9] Cons. 99 : Les grands modèles d'IA génératifs sont un exemple typique d'un modèle *GPAI*, étant donné qu'ils permettent la production flexible de contenus, tels que du texte, de l'audio, des images ou de la vidéo, qui peuvent aisément s'adapter à un large éventail de tâches distinctes.

C'est pourquoi certains modèles sortent du champ d'application des modèles *GPAI* en raison de cette exception, notamment ceux qui sont entraînés spécifiquement pour des tâches telles que la transcription de la parole en texte, la génération de parole à partir d'un texte, l'augmentation de la résolution d'une image, la reconstruction de parties endommagées d'images ou encore la génération de musique sur la base de messages textuels.

En ce qui concerne le cycle de vie du modèle, celui-ci commence véritablement au début du grand cycle de pré-entraînement. Tout développement ultérieur du modèle en aval de cette étape fait partie intégrante du cycle de vie de ce même modèle, plutôt que de donner naissance à un nouveau modèle. Plusieurs exemples de scénarios illustrant les interactions entre les différents rôles gérant des SIA en aval et exploitant des modèles *GPAI* ont d'ailleurs été fournis pour clarifier ces dynamiques.

De plus, des informations détaillées ont été apportées concernant les modifications susceptibles de justifier qu'un modificateur en aval soit également considéré comme un fournisseur des modèles *GPAI*. La condition requise est que **la modification entraîne un changement important de la généralité, des capacités ou du risque systémique du modèle**.

Le critère établi pour satisfaire à cette condition est d'avoir utilisé, pour cette modification, une **puissance de calcul supérieure à un tiers de celle utilisée pour l'entraînement du modèle original**. Dans le cas où la puissance de calcul utilisé pour l'entraînement du modèle initial n'est pas connue, un tiers du seuil indicatif des modèles *GPAI* peut être retenu comme référence.

Si les modifications proposées remplissent cette condition, le fournisseur en aval devra assumer les obligations incombant aux fournisseurs, mais uniquement pour la partie complémentaire ajoutée dans le cadre de ce réglage fin (*fine-tuning*), par exemple en documentant les nouvelles sources de données.

Enfin, d'autres exceptions à l'application de ces obligations ont été prévues, notamment pour les modèles publiés sous des licences libres et ouvertes.

SYSTÈME D'IA

Définitions RIA – Article 3

1) **« système d'IA** (SIA) » : un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels.

Définitions techniques

Tout système doté de **capacités d'inférence** est considéré comme un SIA. Cette capacité d'inférence, dans ce contexte, est identifiée par la concomitance de deux conditions (Cons. 12) :

- la présence d'un **processus consistant à générer des sorties** telles que des prédictions, du contenu, des recommandations ou des décisions, qui peuvent influencer l'environnement physique ou virtuel ;
- la capacité des systèmes d'IA à **inférer des modèles ou des algorithmes**, ou les deux, à partir d'entrées ou de données.

Cette formulation inclut les **IA basées sur l'apprentissage** (*Machine Learning*) et les **IA symboliques**.

Analyse du Hub France IA : Dans sa formulation actuelle, la définition inclut tous les systèmes dont le comportement résulte d'un processus d'apprentissage sur un ensemble de données initiales : régressions linéaires et logistiques, arbres de décision, réseaux de neurones, modèles LLM, etc. Les systèmes à base de connaissances ou de logique, par exemple les IA symboliques, sont également inclus.

Cette définition est indépendante des méthodes d'apprentissage utilisées. Les systèmes qui ont la possibilité d'évoluer en production (*self learning capabilities*), en utilisant les données les plus récentes collectées, sont également inclus dans cette catégorie. Toutefois, les modifications conceptuelles du modèle, du périmètre ou de l'utilisation qui n'étaient pas prévues à l'origine doivent être traitées comme un nouveau système (cf. modification substantielle).

Les SIA sont conçus pour fonctionner à différents niveaux d'autonomie, ce qui signifie qu'ils bénéficient d'un certain degré d'indépendance dans leur action par rapport à une ingérence humaine et de capacités à fonctionner sans intervention humaine.

Les lignes directrices finalisées par la Commission européenne le 29 juillet 2025 apporte des éclaircissements sur la qualification de SIA. Ce document détaille les 7 critères définis pour qualifier un système, tout en fournissant des exemples concrets et des exclusions. On notera un intérêt pratique particulier pour les précisions concernant la capacité d'inférence et, par extension, la liste des systèmes qui ne doivent pas être qualifiés comme tels (voir section 5.2 Systèmes qui ne relèvent pas de la définition du « SIA »).

RISQUES

Définitions RIA – Article 3

2) **« risque » :** la combinaison de la probabilité d'un préjudice et de la sévérité de celui-ci.

Définitions techniques

Le RIA prévoit 4 catégories pour classer les SIA en fonction de leur niveau de risque :

- **SIA interdits** (Art. 5) : l'utilisation de ces systèmes n'est pas autorisée, le risque associé à leur utilisation étant inacceptable ;
- **SIA à haut risque** (Art. 6) : il s'agit du niveau de risque pour lequel le RIA prévoit le plus d'exigences, en matière de documentation, de qualité des données, de performance, de sécurité, de mise en place d'un système de gestion et d'atténuation des risques et présence d'un contrôle humain dans le système.
- **SIA avec obligations particulières de transparence** (Art. 50) : exigences en matière de transparence pour l'utilisateur.
- **SIA à risque minime** : pas d'obligations.

Les deux premières catégories sont au cœur du présent règlement et sont définies par énumération, l'une à l'article 5, l'autre à l'article 6.1 et dans les Annexes I et III : une liste de cas entrant dans ces catégories a été établie et est susceptible d'être modifiée à l'avenir. Les deux dernières catégories ne sont pas explicitement définies par le règlement mais sont déduites de manière résiduelle.

Analyse du Hub France IA : La notion de risque doit être appréciée en fonction des impacts sur la santé, la sécurité, les droits fondamentaux des personnes (définis dans la Charte des droits fondamentaux de l'UE), ou d'autres aspects relatifs à la protection de l'intérêt public.

Sur les 445 occurrences du terme « risque » dans les articles du RIA, 305 concernent l'expression « haut risque », 1 le risque de préjudice, 31 le risque systémique et 6 le risque au sens de l'article 79 « procédure applicable au niveau national aux systèmes d'IA présentant un risque ».

Enfin, une définition de la manière de calculer le risque est considérée comme une condition préalable fondamentale au lancement d'un projet.

Il est important de souligner que les lignes directrices clarifiant la classification des SIA comme « systèmes interdits » ont été finalisées par la Commission le 29 juillet 2025. Par ailleurs, il faut noter que ces catégories ne sont pas cloisonnées : les exigences peuvent être cumulatives. Pour offrir une vision claire de ce point complexe, un feuillet spécifique a été publié afin d'illustrer les différents scénarii possibles lors du déploiement d'un système (voir section « RIA: différents scénarii de classification »).

PERFORMANCES D'UN SYSTÈME D'IA

Définitions RIA – Article 3

18) **« performance d'un SIA » :** la capacité d'un SIA à remplir sa destination.

Définitions techniques

Les performances d'un SIA sont généralement mesurées par différentes **métriques quantitatives**, qui sont utilisées pour évaluer la capacité d'un système à atteindre son objectif ou à résoudre la tâche qu'il s'est fixée. Ces mesures peuvent être fondées sur le jugement d'un expert pour répondre aux besoins spécifiques du système ou sur des mesures statistiques plus classiques que l'on peut trouver dans la littérature scientifique.

Ces métriques sont essentielles à la fois pour la **modélisation** et pour la **surveillance du système** en production. À la définition des métriques doit s'ajouter la sélection d'un *benchmark* qui doit être établi (littérature technique, besoin de l'entreprise, spécificité du cas d'usage, etc).

Analyse du Hub France IA : La sélection des métriques peut se faire selon les critères suivants :

- nature du problème (classification, régressions, etc.) ;
- type de données (structurées, non structurées) ;
- niveau d'interprétabilité requis ;
- exigences métier…

MODIFICATION SUBSTANTIELLE

Définitions RIA – Article 3

23) **« modification substantielle » :** une modification apportée à un SIA après sa mise sur le marché ou sa mise en service, qui n'est pas prévue ou planifiée dans l'évaluation initiale de la conformité réalisée par le fournisseur et qui a pour effet de nuire à la conformité de ce système aux exigences énoncées au chapitre III, section 2, ou qui entraîne une modification de la destination pour laquelle le SIA a été évalué.

Définitions techniques

La notion de « modification substantielle » est utilisée par le RIA en référence aux SIA à haut risque (Cons. 177). Elle identifie chaque modification, non prévue lors de l'évaluation de la conformité **ou non attendue** à l'origine, appliquée après le déploiement d'un SIA et se décline en deux aspects principaux :

- **changement de conception :** comme un changement dans l'architecture du système, un recalibrage du modèle ou un changement du processus de calibrage (prétraitement des données, *feature engineering*, processus d'optimisation, etc.), qui n'aurait pas été envisagé lors de l'évaluation de la conformité ;
- **changement de destination/utilisation/process,** comme l'évolution du périmètre d'application, l'application du système à différents cas d'usage, etc.

Ce changement peut être déclenché par une évolution imprévue du contexte ou une dégradation inattendue des performances du système.

Une modification substantielle doit être communiquée au régulateur et enregistrée dans la base de données de l'UE (Cons. 131). Enfin, **la soumission d'une nouvelle évaluation de la conformité pourrait être nécessaire** (Cons. 128).

Analyse du Hub France IA : Il est important de souligner que l'on peut s'attendre à des évolutions du modèle conformément à sa conception (par exemple, apprentissage en ligne ou apprentissage par renforcement). Étant donné que ces évolutions ont été prises en compte lors de la phase de conception et documentées (annexe IV, point 2.f), elles ne seront pas considérées comme des modifications substantielles.

Le règlement ne fournit pas de détails sur les cas relevant de cette définition. Selon l'interprétation du HFIA, une modification telle que le recalibrage d'un modèle prévu au moment d'une dégradation des performances ne serait pas considérée comme une modification substantielle, si elle avait été anticipée au moment du développement et des mesures correctives appropriées ont été définies dans le cadre du processus de surveillance.

En ce qui concerne les modèles d'IA à usage général (GPAI), avec la publication le 10 juillet 2025 de lignes directrices dédiées, des informations détaillées ont été apportées concernant les modifications qui pourraient justifier qu'un modificateur en aval soit également considéré comme un fournisseur du modèle GPAI (Art. 25 1.b).

Enfin, les événements enregistrés par le système (journalisation) doivent être utilisés pour évaluer la nécessité de déployer une modification substantielle.

HUB FRANCE IA

RIA – Définitions clés

DONNEES BIOMETRIQUES

Définitions RIA – Article 3

34) **« données biométriques » :** les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, telles que des images faciales ou des données dactyloscopiques.

Définitions techniques

Les « données biométriques » incluent des données telles que le visage, les mouvements oculaires, la forme du corps, la voix, la prosodie, la démarche, la posture, le rythme cardiaque, la pression sanguine, l'odeur et la frappe au clavier. L'usage de données biométriques est une caractéristique sensible dans la détermination du niveau de risque d'un SIA.

Analyse du Hub France IA : Selon les considérants du RIA, les données biométriques peuvent permettre des fonctions d'authentification, d'identification ou de catégorisation des personnes physiques, ainsi que de reconnaissance de leurs émotions (Cons. 14[1]).

- Fonction d'identification biométrique : exploitation automatisée de caractéristiques physiques, physiologiques et comportementales (les données biométriques) d'une personne, aux fins d'établir l'identité d'une personne par comparaison des données biométriques de cette personne avec les données biométriques des personnes stockées dans une base de données de référence (comparaison 1-à-plusieurs – « Qui êtes-vous ? » - Cons. 15). L'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives **est interdite**, sauf si et dans la mesure où cette utilisation est strictement nécessaire eu égard à l'un des objectifs indiqués à l'Article 5 1.h du RIA et autorisée par le droit de l'Union ou le droit national (Annexe III). Il convient de noter que la définition même de système d'identification biométrique à distance donnée dans le RIA ne met pas tant l'accent sur la distance que sur l'absence de **participation active** de la part du sujet.

- Fonction de vérification biométrique : ce qui inclut l'authentification (comparaison 1-à-1 - « Êtes-vous bien cette personne ? ») : confirmation qu'une personne physique donnée est bien celle qu'elle prétend être dans le seul but d'avoir accès à un service, de déverrouiller un dispositif ou de disposer d'un accès sécurisé à des locaux. La fonction ne serait **pas interdite ni à haut risque**, considérant que la personne a donné son consentement pour être authentifiée (Cons. 15, Annexe III).

- Fonction de catégorisation biométrique : définie comme le classement de personnes physiques dans certaines catégories sur la base de leurs données biométriques. Ces catégories spécifiques peuvent concerner des aspects tels que le sexe, l'âge, la couleur des cheveux, la couleur des yeux, les tatouages, les traits liés au comportement ou à la personnalité, la langue, la religion, l'appartenance à une minorité nationale ou encore l'orientation sexuelle ou politique (Cons. 16). Cette fonction est classée comme **interdite** sauf dans le domaine répressif pour l'étiquetage ou le filtrage d'ensembles de données biométriques acquis légalement (Art .5 1.g). Dans ce cas, si le droit de l'Union ou le droit national l'autorise, la fonction est considérée comme à **haut risque** (Annexe III).

- Fonction de reconnaissance des émotions : un système d'IA permettant la reconnaissance ou la déduction des émotions ou des intentions de personnes physiques sur la base de leurs données biométriques. L'utilisation de ces systèmes d'IA pour inférer les émotions d'une personne physique sur le lieu de travail et dans les établissements d'enseignement **est interdite**, sauf lorsque l'utilisation du système d'IA est destinée à être mise en place ou mise sur le marché pour des raisons médicales ou de sécurité (Art .5 1.g); Dans les autres cas, cette fonction est considérée comme à **haut risque** (Annexe III).

[1] *Malgré le renvoi du considérant 14 du RIA à la définition de données biométriques donnée par le RGPD (Art 4. 14), il est à noter que cette dernière intègre dans la notion la fonction de « identification unique » que ces données devraient permettre ou confirmer, ce qui n'est pas le cas dans le RIA.*

MODELE D'IA A USAGE GENERAL

Définitions RIA – Article 3

63) **« modèle d'IA à usage général » :** un modèle d'IA, y compris lorsque ce modèle d'IA est entraîné à l'aide d'un grand nombre de données utilisant l'auto-supervision à grande échelle, qui présente une généralité significative et est capable d'exécuter de manière compétente un large éventail de tâches distinctes, indépendamment de la manière dont le modèle est mis sur le marché, et qui peut être intégré dans une variété de systèmes ou d'applications en aval, à l'exception des modèles d'IA utilisés pour des activités de recherche, de développement ou de prototypage avant leur mise sur le marché.

Définitions techniques

Le RIA prévoit des règles pour les modèles d'IA à usage général (*GPAI*) et des règles supplémentaires plus spécifiques pour ceux qui présentent des risques systémiques. Ces règles doivent également s'appliquer lorsque ces modèles sont intégrés dans un SIA ou en font partie. Les obligations incombant aux **fournisseurs de ces modèles d'IA** doivent s'appliquer au plus tard lors de la mise sur le marché de ces modèles. Les fournisseurs de modèles *GPAI* doivent se conformer aux **obligations** suivantes (Art. 53) :

- établir et tenir à jour la documentation technique du modèle, y compris son processus d'entraînement et d'essai et les résultats de son évaluation. Les détails sont fournis à l'Annexe XI du RIA ;
- respecter les lois européennes sur les droits d'auteur ;
- fournir les informations présentant les données utilisées pour entraîner le modèle *GPAI*. La granularité sera fournie par le Bureau de l'IA ;
- élaborer, tenir à jour et mettre à la disposition des **fournisseurs de SIA**, qui ont l'intention d'intégrer le modèle *GPAI* dans leurs SIA, la documentation leur permettant de bien comprendre les capacités et les limites du modèle *GPAI*. Les détails sont fournis à l'Annexe XII du RIA.

Des exceptions à certaines exigences peuvent être faites pour les modèles open source, sauf s'ils présentent un risque systémique.

Ces obligations s'appliquent ici aux **fournisseurs de ces modèles d'IA** car ni les fournisseurs de systèmes d'IA ni les déployeurs ne sont en capacité d'avoir accès à ces informations.

Analyse du Hub France IA : la définition se fonde sur les principales caractéristiques fonctionnelles d'un modèle *GPAI*, en particulier la généralité et la capacité d'exécuter de manière compétente un large éventail de tâches distinctes. Ces modèles sont généralement entraînés avec de grandes quantités de données. Les modèles *GPAI* peuvent être mis sur le marché de différentes manières, peuvent être modifiés ou affinés et ainsi se transformer en nouveaux modèles. Ils ne constituent pas en eux-mêmes des SIA mais ils en sont des composants essentiels incluant d'autres composants, tels qu'une interface utilisateur, pour devenir des SIA (Cons. 97).

Quelques exemples connus de modèles *GPAI* sont les modèles GPT, Claude, Llama et Mistral. Ces modèles peuvent être utilisés tels quels dans des SIA (ex: Copilot) ou intégrés dans des SIA après *fine-tuning*, *RAG*, etc.

La régulation de ces modèles est apparue tardivement dans le processus d'élaboration du RIA, ce qui explique **l'approche différenciée** pour la régulation de ces modèles par rapport aux SIA prédictifs. Cela est dû à la diffusion de cette technologie au grand public fin 2022.

MODELE D'IA A USAGE GENERAL

Analyse du Hub France IA : le 10 juillet 2025 a été publié le Code de bonnes pratiques, un cadre d'application volontaire visant à faciliter la mise en conformité des fournisseurs d'IA avec les obligations du RIA en matière de transparence, de droits d'auteur et de sécurité. Ce Code est assorti de lignes directrices applicatives essentielles qui dissipent de nombreuses zones d'ombre quant à la définition des rôles des différents acteurs impliqués, aux critères de qualification d'un modèle *GPAI* et aux obligations qui s'y rattachent.

Pour établir cette classification, le document s'appuie fondamentalement sur le considérant 98, précisant qu'un modèle doté d'au moins un milliard de paramètres et entraîné sur un vaste ensemble de données présente une généralité significative, ainsi que sur le considérant 99, qui désigne les grands modèles d'IA génératifs comme des exemples typiques de modèles *GPAI*.

L'approche adoptée par la Commission repose sur l'évaluation de la « **puissance de calcul utilisée pour l'entraînement** », un indicateur pertinent puisqu'il combine les deux notions complémentaires que sont le nombre de paramètres et le nombre d'exemples d'entraînement qui soit raisonnablement aisé à estimer par les fournisseurs. Ainsi, un seuil indicatif a été fixé à 10^{23} flops pour identifier un modèle *GPAI*, à condition que le modèle soit également capable de générer du langage, ou de produire des images ou des vidéos à partir d'un texte.

Toutefois, même si un modèle remplit ces critères quantitatifs, une exception reste applicable s'il est avéré qu'**il ne présente pas une généralité significative** ou qu'**il n'est pas capable d'exécuter** de manière compétente **un large éventail de tâches distinctes**. C'est pourquoi certains modèles sortent du champ d'application des modèles *GPAI* en raison de cette exception, notamment ceux qui sont entraînés spécifiquement pour des tâches telles que la transcription de la parole en texte, la génération de parole à partir d'un texte, l'augmentation de la résolution d'une image, la reconstruction de parties endommagées d'images, ou encore la génération de musique sur la base de messages textuels.

En ce qui concerne le cycle de vie du modèle, celui-ci commence véritablement au début du grand cycle de pré-entraînement. Tout développement ultérieur du modèle en aval de cette étape fait partie intégrante du cycle de vie de ce même modèle, plutôt que de donner naissance à un nouveau modèle. Plusieurs exemples de scénarios illustrant les interactions entre les différents rôles gérant des SIA en aval et exploitant des modèles *GPAI* ont d'ailleurs été fournis pour clarifier ces dynamiques.

De plus, des informations détaillées ont été apportées concernant les modifications qui pourraient justifier qu'un modificateur en aval soit également considéré comme un fournisseur de modèle *GPAI*. La condition requise est que **la modification entraîne un changement important de la généralité, des capacités ou du risque systémique du modèle**. Le critère établi pour satisfaire à cette condition est d'avoir utilisé, pour cette modification, **une puissance de calcul supérieure à un tiers de celle utilisée pour l'entraînement du modèle original**. Dans le cas où la puissance de calcul de l'entraînement du modèle initial n'est pas connue, un tiers du seuil indicatif des modèles *GPAI* peut être retenu comme référence.

Si les modifications proposées remplissent cette condition, le fournisseur en aval devra assumer les obligations incombant aux fournisseurs, mais uniquement sur la partie complémentaire ajoutée dans le cadre de ce réglage fin (*fine-tuning*), par exemple, en documentant les nouvelles sources de données.

Enfin, d'autres exceptions à l'application de ces obligations ont été prévues, notamment pour les modèles publiés sous des licences libres et ouvertes.

HUB FRANCE IA

RIA– Définitions clés

RISQUE SYSTEMIQUE

Définitions RIA – Article 3

65) **« risque systémique » :** un risque spécifique aux capacités à fort impact* des modèles *GPAI*, ayant une incidence significative sur le marché de l'Union en raison de leur portée ou d'effets négatifs réels ou raisonnablement prévisibles sur la santé publique, la sûreté, la sécurité publique, les droits fondamentaux ou la société dans son ensemble, pouvant être propagé à grande échelle tout au long de la chaîne de valeur.

*64) **« capacités à fort impact » :** des capacités égales ou supérieures aux capacités enregistrées dans les modèles *GPAI* les plus avancés.

Définitions techniques

Un modèle est présumé présenter un tel risque (à fort impact) lorsqu'il dépasse 10^{25} opérations en virgule flottante pendant la phase d'entraînement. Le nombre d'opérations utilisées dans le processus de formation est l'un des indicateurs, mais ce n'est pas le seul. La Commission pourra également déterminer qu'un modèle d'IA présente un risque systémique en se basant soit sur une alerte qualifiée du groupe scientifique ou sur la base d'autres critères, dont le nombre de paramètres utilisés, la taille de l'ensemble de données impliquées dans le processus de modélisation, le type de données d'entrée/sortie (texte, images, multimodal), l'impact sur le marché de l'Union et le nombre d'utilisateurs (Annexe XIII). Les critères et les seuils actuellement indiqués dans le RIA **pourraient évoluer** à l'avenir en fonction des progrès technologiques par actes délégués (Art. 51). Dès lors qu'un modèle *GPAI* remplit ces conditions, le fournisseur concerné doit en **informer la Commission** (Art. 52).

Les fournisseurs de modèles *GPAI* présentant des risques systémiques sont soumis, en plus des obligations prévues pour les fournisseurs de modèles *GPAI*, à **des exigences supplémentaires** d'évaluation, de transparence et de cybersécurité définies à l'Article 55. La conformité à ces exigences peut être démontrée par l'application des codes de bonnes pratiques prévus à l'article 56. Elle est présumée lorsque la norme européenne harmonisée est respectée.

Analyse du Hub France IA : Les modèles *GPAI* à risque systémique sont présumés **plus risqués** que les modèles *GPAI* classiques. En effet, les risques augmentent avec la taille (nombre de paramètres du modèle), la nature de l'ensemble de données, le nombre d'utilisateurs, etc. Par exemple, un ensemble de données plus grand contiendra potentiellement plus de données protégées, un modèle plus grand aura un impact environnemental plus élevé et plus d'utilisateurs peuvent avoir plus d'impacts négatifs.

Le 10 juillet 2025 a été publié le Code de bonnes pratiques , un cadre d'application volontaire visant à faciliter la mise en conformité des fournisseurs d'IA avec les obligations du RIA en matière de transparence, de droits d'auteur et de sécurité. Ce Code est assorti de lignes directrices applicatives essentielles qui dissipent de nombreuses zones d'ombre quant à la définition des rôles des différents acteurs impliqués, aux critères de qualification d'un modèle *GPAI* et aux obligations qui s'y rattachent.

SYSTEME D'IA A USAGE GENERAL

Définitions RIA – Article 3

66) **« système d'IA à usage général » :** un SIA qui est fondé sur un modèle *GPAI* et qui a la capacité de répondre à diverses finalités, tant pour une utilisation directe que pour une intégration dans d'autres SIA.

Définitions techniques

Un « SIA à usage général » est un modèle fondé sur un modèle *GPAI*. Comme tout SIA, il doit être qualifié au regard des trois catégories de risques identifiées par le RIA. En fonction des circonstances, les différents acteurs de la chaîne de valeurs de ces systèmes (par exemple, fournisseur du modèle *GPAI* et déployeur du SIA à usage général) doivent clarifier leurs rôles et responsabilités respectives pour permettre le respect des obligations applicables (Art. 25).

Analyse du Hub France IA : le fournisseur des SIA à usage général devra être très vigilant sur la **répartition des responsabilités** entre lui et le fournisseur du modèle *GPAI*.

Quelques exemples sont *Chat-GPT, Dall-E* et *Gemini*, et des SIA à usage général développés par les entreprises.

FINALITE ET DESTINATION

Définitions RIA – Article 3

12) **« destination » :** l'utilisation à laquelle un SIA est destiné par le fournisseur, y compris le contexte et les conditions spécifiques d'utilisation, tels qu'ils sont précisés dans les informations communiquées par le fournisseur dans la notice d'utilisation, les indications publicitaires ou de vente et les déclarations, ainsi que dans la documentation technique.

Le terme «finalité » n'est pas définit en tant que tel dans le RIA, mais il est présent dans la définition d'un SIA à usage général : «un système d'IA qui est fondé sur un modèle *GPAI* et qui a la capacité de répondre **à diverses finalités**, tant pour une utilisation directe que pour une intégration dans d'autres SIA ».

Définitions techniques

Les fournisseurs devront définir la ou les destinations du SIA en établissant un cadre général des usages possibles, permettant au déployeur de l'utiliser selon ses besoins spécifiques. Ils doivent également anticiper les utilisations du SIA qui peuvent être raisonnablement prévisibles en raison de comportements humains dans le contexte des caractéristiques et de l'utilisation du système, afin que le déployeur en prenne connaissance et en tienne compte lors de son utilisation.

Exemple : *un outil de transcription automatique « speech to text » pour des réunions professionnelles.*

Les déployeurs devront définir la ou les finalités d'usage en fonction des besoins qu'ils souhaitent satisfaire avec le SIA, puis l'utiliser en conséquence, dans le respect de la ou des destinations initiales définies par le fournisseur.

Exemple : *une entreprise utilise l'outil de transcription automatique pour générer des procès-verbaux de réunions internes, tandis qu'un journaliste l'utilise pour retranscrire des interviews.*

Analyse du Hub France IA : si la « destination » du SIA est clairement définie et répond d'un cadre strict [mention à indiquer obligatoirement par le fournisseur au sein de la documentation technique ainsi que dans d'autres supports±, le RIA est moins précis sur la question de la « finalité ». Ce terme est mentionné à once reprises dont trois en référence au RGDP concernant la finalité du traitement de données. Dans les autres cas, il s'agit d'une référence aux besoins du déployeur.

L'articulation entre notions de destination et de finalité n'est pas dépourvue de liens et dépendra largement de l'étape du projet à laquelle on se situe :

- **l'expression d'un besoin** conduira en premier lieu à déterminer la finalité pour laquelle il est souhaité recourir à un SIA. La finalité pourra être amenée à évoluer au cours de la définition du projet ;
- **le développement** du SIA impliquera nécessairement quant à lui d'en définir la destination qui conditionnera la finalité pour laquelle le déployeur va l'utiliser. Toute modification de la destination d'un SIA constitue un nouveau produit qui devra répondre au cadre de conformité correspondant (qualification de l'opérateur, du SIA, identification des obligations).

QUALIFICATION DES ACTEURS

Définitions RIA – Article 3

3) "**fournisseur**", une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe ou fait développer un système d'IA ou un modèle d'IA à usage général et le met sur le marché ou met le système d'IA en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit;

4) "**déployeur**", une personne physique ou morale, une autorité publique, une agence ou un autre organisme utilisant sous sa propre autorité un système d'IA sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnel;

Définitions techniques

Le **fournisseur** est celui qui crée, ou fait créer, un système ou un modèle d'IA et qui le met sur le marché sous son propre nom ou sa propre marque. C'est le rôle qui comporte le plus de responsabilités légales : il doit, entre autres, garantir que le système est conforme aux règles, rédiger la documentation technique, enregistrer le système et apposer le marquage CE. Le **déployeur** est celui qui utilise le système sous sa propre autorité, dans son organisation ou son activité.

La différence centrale est donc simple : le fournisseur répond principalement de la **conformité du système**, tandis que le déployeur répond de son **usage concret**. L'usage purement personnel et non professionnel est exclu de la notion de déployeur.

Analyse du Hub France IA : Pour les SIA à haut risque, la distinction se traduit par deux blocs d'obligations. Le fournisseur porte la responsabilité principale de la conformité du système avant et pendant sa mise sur le marché ou sa mise en service : il doit mettre en place un système de gestion de la qualité, conserver la documentation, tenir les journaux lorsqu'ils sont sous son contrôle, soumettre le système à l'évaluation de conformité, établir la déclaration UE, apposer le marquage CE, procéder à l'enregistrement, prendre les mesures correctives nécessaires et fournir aux autorités les éléments permettant de démontrer la conformité. Le déployeur, lui, est responsable de l'usage concret du système : il doit l'utiliser conformément à la notice, confier le contrôle humain à des personnes compétentes, veiller à la qualité des données d'entrée lorsqu'il les contrôle, surveiller le fonctionnement, conserver les journaux sous son contrôle et, en cas de risque ou d'incident grave, informer les acteurs compétents et, le cas échéant, suspendre l'utilisation du système.

Un utilisateur (ou tout autre tiers) devient légalement "fournisseur" s'il modifie de façon substantielle un système à haut risque, s'il change son usage prévu pour le rendre « à haut risque », ou s'il appose son propre nom sur un système existant. À l'inverse, l'usage purement personnel et non professionnel, ainsi que la recherche scientifique avant la mise sur le marché, sont exclus de ces obligations (art. 25).

QUALIFICATION DES ACTEURS

Définitions RIA – Article 3

5) "**mandataire**", une personne physique ou morale située ou établie dans l'Union ayant reçu et accepté un mandat écrit d'un fournisseur de système d'IA ou de modèle d'IA à usage général pour s'acquitter en son nom des obligations et des procédures établies par le présent règlement;

6) "**importateur**", une personne physique ou morale située ou établie dans l'Union qui met sur le marché un système d'IA qui porte le nom ou la marque d'une personne physique ou morale établie dans un pays tiers;

7) "**distributeur**", une personne physique ou morale faisant partie de la chaîne d'approvisionnement, autre que le fournisseur ou l'importateur, qui met un système d'IA à disposition sur le marché de l'Union;

Définitions techniques

Ces trois rôles servent à encadrer la mise sur le marché quand l'IA vient de l'étranger ou passe par des intermédiaires.

Le **mandataire** est le représentant officiel, basé dans l'Union européenne, désigné par un fournisseur situé en dehors de l'UE. Il sert de point de contact pour les autorités européennes et doit s'assurer que toute la documentation est disponible. S'il constate que le fournisseur ne respecte pas les règles, il doit rompre son contrat avec lui.

L'**importateur** est l'acteur basé dans l'UE qui commercialise une IA fabriquée hors de l'UE. Son rôle est de vérifier que le fournisseur a bien respecté la loi (marquage CE, documentation, désignation d'un mandataire) avant de lancer la vente.

Le **distributeur** est tout intermédiaire commercial qui vend le système sur le marché. Il effectue un contrôle de base (présence du marquage CE et des instructions) et doit cesser la vente s'il a un doute sur la conformité.

Analyse du Hub France IA : Si un importateur ou un distributeur appose son propre nom sur un système d'IA à haut risque, il devient alors légalement le fournisseur de ce système.

QUALIFICATION DES ACTEURS

Définitions RIA – Article 3

8) "**opérateur**", un fournisseur, fabricant de produits, déployeur, mandataire, importateur ou distributeur;

58) "**participant**", aux fins des essais en conditions réelles, une personne physique qui participe à des essais en conditions réelles;

68) "**fournisseur en aval**", un fournisseur d'un système d'IA, y compris d'un système d'IA à usage général, qui intègre un modèle d'IA, que le modèle d'IA soit fourni par lui-même ou non, et verticalement intégré ou fourni par une autre entité sur la base de relations contractuelles.

Définitions techniques

L'**opérateur** n'est pas un rôle autonome : c'est une catégorie globale qui regroupe fournisseur, fabricant de produits, déployeur, mandataire, importateur et distributeur. Elle sert à désigner collectivement les acteurs soumis au règlement. Un même acteur peut donc cumuler plusieurs qualités, par exemple être à la fois importateur et distributeur.

Le **participant** n'est pas un opérateur économique : c'est la personne physique qui prend part à des essais en conditions réelles. Son rôle appartient à la phase expérimentale du cycle de vie. Les essais en conditions réelles ne constituent pas une mise sur le marché ni une mise en service si les conditions prévues par le règlement sont respectées.

Le **fournisseur en aval** est le fournisseur d'un système d'IA qui intègre un modèle d'IA, qu'il l'ait développé lui-même ou qu'il l'ait reçu d'une autre entité. C'est un rôle clé dans les architectures modernes : le sujet réglementé n'est pas seulement celui qui entraîne le modèle, mais aussi celui qui l'intègre dans une application ou un système destiné à un usage concret.

Analyse du Hub France IA : un modèle général devient souvent juridiquement pertinent lorsqu'il est intégré dans un produit, un service ou un processus déterminé. Le fournisseur en aval doit donc comprendre les capacités, les limites et les risques du modèle qu'il utilise, même lorsqu'il ne l'a pas conçu.

C'est pourquoi l'article 53 impose aux fournisseurs de modèles d'IA à usage général de fournir une documentation suffisante aux acteurs qui souhaitent intégrer ces modèles dans leurs propres systèmes. Cette documentation doit permettre au fournisseur en aval de respecter ses obligations, notamment en matière de conformité, de gestion des risques et d'information sur le fonctionnement du système.

HUB FRANCE IA

III. Définition d'un projet

III. DÉFINITION D'UN PROJET

La démarche projet de mise en œuvre du SIA est au cœur du processus d'opérationnalisation du RIA que nous proposons, elle accompagne la mise en conformité d'un SIA tout au long de son cycle de vie. Les grandes étapes de la démarche projet sont représentées en Figure 1. Dans la suite du document, nous décrivons les différentes étapes, les actions à mener, les outils à mettre en place et proposons une *check list* opérationnelle.

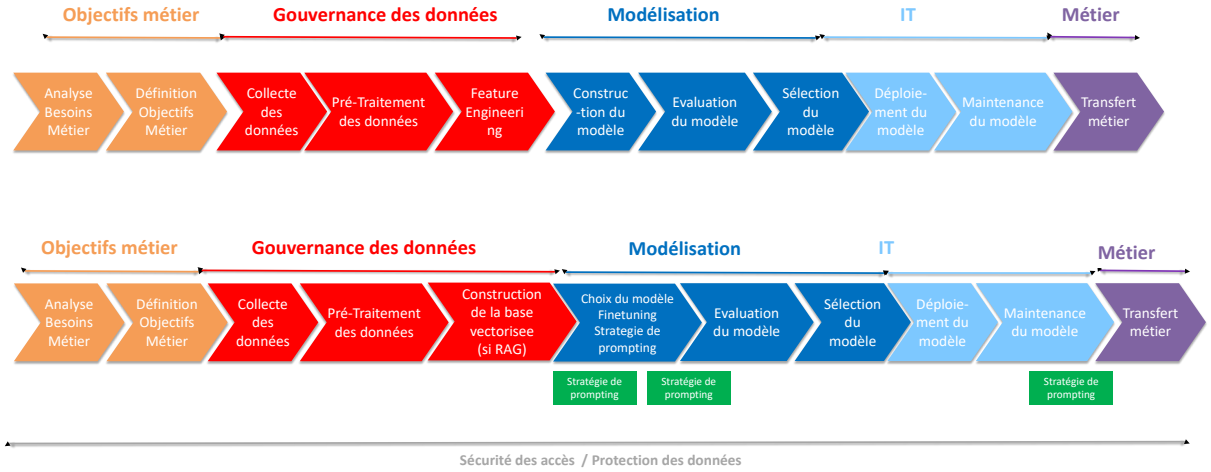


Figure 1 – Démarche projet de mise en œuvre d'un SIA (IA prédictive en haut et IA générative en bas)

III.1 INTRODUCTION

La phase de définition d'un projet constitue la première phase du cycle de vie de la conception d'un SIA. À ce stade, les contours du projet sont encore en cours de structuration : il n'est notamment pas encore arrêté si le SIA sera développé en interne ou acquis auprès d'un prestataire externe.

Ce choix, souvent perçu comme opérationnel ou budgétaire, revêt en réalité une importance déterminante au regard de la conformité réglementaire. Il emporte en effet un double impact :

- sur la qualification de l'opérateur au regard de la réglementation applicable ;
- sur les obligations de conformité qui en découlent.

L'analyse proposée par le Hub France IA repose sur un outil structurant : **la fiche projet**. Initiée dès cette phase de définition du projet, elle **doit être maintenue à jour tout au long du cycle de vie**.

La phase de définition débute par l'identification et le tri des projets ou cas d'usage potentiels. Cette étape vise à formaliser les premières hypothèses structurantes du projet : finalité poursuivie, périmètre fonctionnel envisagé, données mobilisées, parties prenantes impliquées et modalités de mise en œuvre.

Ces premiers arbitrages conditionnent la qualification juridique ultérieure du système et orientent les analyses qui seront menées dans les étapes suivantes.

Si la phase de définition intervient en amont du projet, elle ne disparaît pas pour autant une fois celui-ci lancé. Toute évolution significative du périmètre, des fonctionnalités ou des modalités de mise en œuvre doit conduire à réexaminer les éléments formalisés à ce stade. Toute modification au projet nécessite une revue de la phase de « définition du projet », afin de déterminer si elle est « substantielle » et si elle modifie certains éléments de la fiche projet.

III.2 Ideation

La phase d'idéation constitue la première étape de la définition du projet. Elle a pour objectif de faire émerger un ensemble de cas d'usage susceptibles d'être adressés par des solutions d'IA.

Il est essentiel, à ce stade, d'encourager une génération large et structurée d'idées. Cette dynamique peut s'appuyer sur plusieurs leviers complémentaires :

- des **échanges avec les directions métiers**, permettant d'identifier des cas d'usage concrets à partir des besoins opérationnels, des irritants rencontrés ou des opportunités d'amélioration propres à chaque activité ;
- **l'identification d'évolutions technologiques**, notamment lorsqu'une solution logicielle existante intègre de nouvelles briques d'IA susceptibles d'ouvrir des perspectives d'usage inédites au sein de l'organisation.

Cette phase comporte toutefois un risque : celui d'une inadéquation entre les capacités réelles des technologies d'IA et les cas d'usage envisagés. Ce décalage résulte fréquemment d'une méconnaissance des techniques mobilisables, de leurs conditions de mise en œuvre ou des risques associés à leur utilisation.

Une démarche d'acculturation aux usages et aux techniques de l'IA apparaît dès lors indispensable. Elle permet de mieux qualifier les opportunités identifiées, d'éviter les effets d'annonce ou les projets mal calibrés et de tirer pleinement parti du potentiel de cette phase d'idéation.

III.3 Priorisation et filtrage

Une fois la phase d'idéation achevée, l'organisation dispose d'un portefeuille élargi de cas d'usage potentiels. L'étape suivante consiste à opérer un tri afin d'identifier les projets qui méritent d'être approfondis.

Cette priorisation repose sur un examen structuré, articulé autour de trois dimensions :

- **l'alignement stratégique et la priorisation :** le cas d'usage envisagé doit s'inscrire dans les objectifs stratégiques de l'entreprise, qu'ils soient financiers, opérationnels, organisationnels ou éthiques. Il s'agit d'évaluer la valeur attendue du projet : amélioration de la performance, optimisation des processus, différenciation concurrentielle, qualité de service ou encore conformité aux engagements éthiques de l'organisation. Cet examen permet non seulement de vérifier la pertinence du projet, mais également de hiérarchiser les initiatives entre elles : les cas d'usage apportant la plus forte valeur au regard des priorités stratégiques doivent être traités en priorité, afin d'allouer efficacement les ressources disponibles ;
- **la pertinence et la proportionnalité du recours à l'IA** : l'IA doit constituer un outil approprié pour atteindre l'objectif poursuivi et ne pas se substituer à une solution plus simple – automatisation classique, optimisation organisationnelle ou traitement statistique – susceptible d'offrir un résultat équivalent. Son utilisation doit en outre présenter un avantage significatif au regard des coûts, des impacts organisationnels, des exigences de gouvernance et des risques associés. Cette appréciation relève d'une logique de proportionnalité : le recours à un SIA doit être justifié par un gain réel et mesurable au regard du but recherché ;
- **l'absence d'interdiction manifeste** : dès cette étape, un premier contrôle doit être opéré afin de vérifier que le cas d'usage envisagé ne relève pas d'une pratique interdite par le RIA. Ce contrôle préliminaire permet d'éviter d'investir des ressources dans des projets dont la mise en œuvre serait, par principe, prohibée.

III.4 Faisabilite et preanalyse des risques

Cette étape vise à conduire une première analyse structurée des risques associés aux cas d'usage précédemment priorisés. Il ne s'agit pas encore d'une évaluation exhaustive, mais d'une appréciation initiale permettant d'identifier le niveau de vigilance requis et d'anticiper les principales contraintes réglementaires et organisationnelles.

L'analyse porte notamment sur trois dimensions complémentaires :

- **les enjeux éthiques**, au regard des principes d'IA responsable ou d'IA de confiance applicables, notamment ceux adoptés par l'organisation (non-discrimination, explicabilité, supervision humaine, impact sociétal, *etc.*) ;
- **les enjeux juridiques et réglementaires**, en particulier au regard du RIA, afin d'identifier si le système relève potentiellement d'une pratique interdite, d'un SIA à haut risque, d'une catégorie soumise à des obligations spécifiques de transparence ou de la catégorie des SIA génératives intégrant des modèles *GPAI* ;
- **les enjeux techniques et opérationnels**, tels que la disponibilité et la qualité des données, la robustesse attendue du système, sa capacité d'intégration dans l'environnement existant ou encore les besoins en matière de gouvernance.

Sur la base de cette analyse préliminaire, les cas d'usage peuvent être répartis en trois catégories :

- **cas d'usage non retenus** : projets incompatibles avec le cadre réglementaire applicable (par exemple, relevant d'une pratique interdite au sens du RIA) ou contraires aux exigences éthiques et techniques de l'organisation ;
- **cas d'usage à risque significatif** : projets susceptibles de relever d'un régime exigeant (notamment celui applicable aux SIA à haut risque) ou présentant des enjeux éthiques ou techniques sensibles. Ces cas nécessitent la mise en place précoce de mécanismes d'évaluation de l'impact potentiel et de maîtrise des risques (documentation, supervision humaine, gouvernance des données, traçabilité, *etc.*) ;
- **cas d'usage à risque limité** : projets dont le niveau de risque apparaît, à ce stade, modéré. Ils demeurent néanmoins soumis à un suivi proportionné, leur profil pouvant évoluer au cours du cycle de vie.

Cette première qualification permet d'initier, dès la phase de définition, le processus de gestion des risques au sens du RIA et de la politique IA responsable de l'entreprise. Elle n'a pas vocation à figer définitivement le niveau de risque, mais à poser les bases d'un pilotage continu : la gestion des risques doit en effet accompagner le SIA tout au long de son cycle de vie, de la conception au déploiement, puis en phase d'exploitation.

Les SIA relevant de ces catégories sont également susceptibles d'intégrer des modèles *GPAI*, lesquels sont assujettis à ces règles complémentaires spécifiques.

HUB FRANCE .IA

RIA – Opérationnalisation

DÉFINITION D'UN PROJET (1)

A cette étape du cycle projet, l'objectif est d'encourager l'émergence de cas d'usage utilisant de l'IA, par l'identification et le tri des projets potentiels à lancer

Etape 1
Idéation
→ **Lister tous les projets pouvant être adressés par l'IA**

Etape 2
Priorisation Filtrage
→ **Filtrer les projets en fonction de leur pertinence**

Etape 3
Faisabilité Pré-analyse des risques
→ **Déterminer le niveau de risque pressenti des projets**

(1) La Phase et les Etapes font référence au livrable « Opérationnaliser la gestion des risques » du GT Banque du Hub France IA

HUB FRANCE IA

RIA – Opérationnalisation

DÉFINITION D'UN PROJET

1.Idéation

Encourager la génération d'idées et de cas d'usage

- Echanger avec des personnes appartenant à un domaine métier spécifique
- Encourager, par une animation des experts, l'évocation d'irritants ou d'opportunités qui pourraient être adressés par de l'IA

2. Priorisation

Sélectionner les cas d'usage à approfondir

- Aligner les idées avec les objectifs stratégiques de l'entreprise (qu'ils soient financiers ou éthiques)
- Définir la nécessité d'avoir recours aux technologies d'IA et en quoi cela offre-t-il des avantages significatifs
- Attester que le cas d'usage ne relève pas d'une pratique interdite

3. Faisabilité

Analyser de façon rudimentaire les risques associés

- Déterminer un premier niveau de risque sur la base du RIA et de la politique IA responsable/ de confiance de l'entreprise
- Initier le processus de gestion des risques (à faire tout au long du cycle de vie du SIA)

Boite à outils

Session de sensibilisation et d'acculturation à l'IA et à la réglementation

Groupe pluridisciplinaire d'échanges et de réflexion

Template d'informations à collecter pour chaque idée de cas d'usage développée

Politiques internes de l'organisation relatives à la DATA, l'IA et l'éthique/droits fondamentaux

Procédure de sélection des cas d'usage permettant de quantifier la valeur de l'apport de chaque cas d'usage

Questionnaire de pré-analyse des risques du SIA

Outil de suivi des décisions à travers les processus (date, lieu, contributeurs etc.) et les résultats de la sélection

Notre checklist pour vous aider à opérationnaliser le RIA

- ❑ **Liste d'idées**
- ❑ **Fiche projet**(2) – Initialisation

- ❑ **Liste des projets sélectionnés** (Décision de filtrage pour avancement étude projet)
- ❑ **Fiche projet** (2) – Mise à jour
  - Identifier qu'il ne s'agit pas d'un SIA Interdit
  - Arbitrage Go/NoGo d'avancement projet
  - Justification du recours à un SIA

- ❑ **Résultat Triage**
- ❑ **Fiche projet** (2) – Mise à jour
  - Préciser le niveau de risque/criticité du projet par rapport au RIA et aux politiques internes
  - Qualification du rôle de l'organisation
- ❑ **Initiation d'un « registre des risques »** par rapport aux différents principes IA responsable/de confiance qui alimentera le système de gestion des risques

(2) L'explication plus détaillée de la Fiche Projet est disponible dans le **« Langage commun »** livrée par le GT BAIA

HUB FRANCE .IA

RIA– Opérationnalisation

DÉFINITION D'UN PROJET

Le Hub France IA a identifié à ce jour des éléments qui doivent être pris en compte à chacune des étapes de la phase de « définition d'un Projet »

A toutes les étapes

Boîte à outils

- Processus gestion projet de l'organisation;
- Politiques internes de l'organisation relatives à la DATA, l'IA et l'éthique/droits fondamentaux;
- Formations et référentiels de compétences liés à l'IA.

Notre checklist pour vous aider à opérationnaliser le RIA

- ❑ **Registre des décisions**
- ❑ **Définition** de ce qui est considéré comme **un SIA** ou pas *(Art. 3.1, RIA)*
- ❑ **Preuve de formation** d'acculturation IA des salariés sur le domaine visé *(Art.4, Cons.20 RIA)*

III.6 Concept cle : fiche projet

Afin de faciliter le suivi du projet, nous conseillons d'initier, dès la phase de définition du projet, une **fiche projet permettant de formaliser le cadre d'usage du SIA** et d'en assurer le suivi tout au long de son cycle de vie.

Les principaux éléments à documenter dans cette fiche projet sont :

- définition initiale du projet, avec la spécification des objectifs métiers poursuivis ;
- identification des finalités du SIA et, le cas échéant, de sa destination, lorsque l'entreprise intervient en qualité de fournisseur du SIA ;
- identification du niveau de risque, comprenant la justification de l'analyse permettant d'écarter, le cas échéant, la qualification du cas d'usage comme pratique interdite, ainsi que l'estimation du niveau de risque du SIA et, le cas échéant, du modèle *GPAI* intégré ;
- analyse au regard des principes d'IA éthique et responsable et des politiques et référentiels applicables au sein de l'entreprise (RGPD, éthique, IA et données, sécurité, etc.) ;
- qualification du rôle de l'entreprise *vis à vis* du SIA et, le cas échéant, des modèles *GPAI* ;
- analyse des données disponibles et nécessaires à la mise en œuvre du projet ;
- estimation de la valeur apportée par le projet (financière, opérationnelle, sociétale, etc.) ;
- définition d'un plan de surveillance précisant les valeurs, indicateurs et autres éléments de référence à suivre tout au long du projet ;
- relevé de décision d'avancement et des éventuels points d'arbitrage (*Go/NoGo*).

HUB FRANCE IA

RIA – Concepts clés

FICHE PROJET

Contexte et objectifs

La **fiche projet** n'est pas un livrable RIA mais **contient des informations attendues par le RIA.**

Ce document est à la main de l'organisation, et est **itératif** (il peut être tout ou en partie existant dans le cadre d'un processus de gestion de projet IIT en place dans l'organisation).

Son contenu peut servir à alimenter la documentation de la conformité au RIA (cf. les références aux articles et considérant du RIA ci-dessous).

La fiche projet ne remplace pas la documentation juridique et réglementation attendue par le RIA, elle peut néanmoins en être une source d'information.

Proposition de contenu

En tant que **support qui est mis à jour tout au long de la vie du projet d'IA**, la fiche projet pourra contenir les éléments suivants (liste non exhaustive) :

- définition initiale du projet avec spécification des objectifs métiers (art. 3, art. 12 et cons. 27) ;
- justification de l'intérêt de l'usage de l'IA pour ce projet (Cons. 165) ;
- identification des finalités du SIA et le cas échéant sa destination (si fournisseur) (cons. 165) ;
- identification du niveau de risque : préciser qu'il ne s'agit pas d'un SIA INTERDIT (art. 5 + cons. 6) et niveau de risque pressenti du SIA (et du modèle si *GPAI*) (art. 6 et art. 50) ;
- analyse par rapport aux principes IA responsable/de confiance et politiques de l'entreprise applicables (RGPD, RSE, IA et Data, Cyber, Sécurité, …) ;
- qualification du rôle de l'entreprise vis-à-vis du SIA (et du modèle si *GPAI*) (art. 72, cons. 76 et cons. 155) ;
- pré-analyse de la donnée disponible et nécessaire ;
- estimation de la valeur apportée (financière, sociétale, …) ;
- valeurs/KPI à suivre pour donner un cadre de référence tout au long du projet (évaluation performance et qualité) (art. 72) ;
- relevé de décision d'avancement (*Go/NoGo*).

Analyse du Hub France IA : ce document est initié lors de la phase «définition d'un projet » (cf. feuillet dédié), et doit être maintenu à jour.

Toute évolution dans le cadre du projet nécessite une redéfinition des objectifs métiers (mise à jour du cadrage, *Go/NoGo*, définition des nouvelles métriques).

Ce document ne vient pas se substituer aux autres outils/livrables prévus par le RIA et devant être constitués et alimentés aux autres étapes du projet (système de gestion de risques/système de gestion de la qualité, documentation technique, …). Il constitue néanmoins une première étape pour répondre à l'**objectif d'*accountability*.**

HUB FRANCE IA

IV. Objectif métiers

IV. OBJECTIF MÉTIERS

IV.1 INTRODUCTION

Une fois le cas d'usage sélectionné à l'issue des phases de définition, de priorisation et de préanalyse des risques, l'organisation entre dans une étape décisive : la formalisation précise du projet en vue de son lancement. L'enjeu n'est plus d'explorer des opportunités, mais de structurer un projet unique et déterminé, en posant les bases d'une décision éclairée de lancement.

Cette étape cruciale permet de définir clairement les contours et objectifs métiers du projet d'IA sélectionné.

Au cours de cette étape, l'équipe projet travaille à détailler les spécifications techniques, fonctionnelles et opérationnelles du SIA envisagé.

Ce processus inclut la définition des ressources nécessaires, l'établissement d'une calendrier provisionnel, l'identification des principales parties prenantes ainsi que l'élaboration d'un plan de gestion des risques plus détaillé.

Cette spécification approfondie du projet est essentielle pour préparer efficacement son lancement et assurer sa réussite. Elle constitue un point de bascule entre la phase d'analyse et l'entrée effective dans le développement ou l'intégration du SIA.

IV.2 ANALYSE DES BESOINS METIERS

Le succès du projet dépend de son adéquation avec les besoins métiers qui seront associés à ce projet. Il est ainsi nécessaire de cadrer précisément ces besoins au regard des éléments suivants :

- les bénéfices attendus, notamment en matière de performance, de qualité ou d'optimisation des processus ;
- la définition de la finalité attendue du SIA étudié[10], c'est-à-dire le résultat concret qu'il doit produire ou auquel il doit contribuer ;

[10] *Nota bene* : tandis que la destination est définie dans le RIA comme ayant été expressément définie par le fournisseur, la finalité semble correspondre spécifiquement à l'utilisation que va en faire le déployeur., voir fiche définition « Finalité/Destination ».

- la disponibilité et la qualité des données nécessaires à son fonctionnement ;
- la capacité à déployer la solution, tant du point de vue technique qu'organisationnel et opérationnel.

Ce cadrage constitue un préalable indispensable à toute décision de lancement.

IV.3 Decision de lancement

À l'issue de l'analyse des besoins, l'organisation doit procéder à un arbitrage formel sur le lancement du projet. Cette décision repose sur une appréciation consolidée des éléments examinés lors des étapes précédentes : valeur métier attendue, faisabilité technique et organisationnelle, équilibre entre les bénéfices et les risques identifiés, ainsi que disponibilité des ressources humaines et techniques nécessaires.

Lorsque le projet repose sur l'intégration d'un SIA fourni par un tiers, la décision doit également tenir compte des conditions d'utilisation définies par le fournisseur. La finalité retenue pour le système doit être conforme à sa destination prévue et avec les usages autorisés. Le déployeur doit notamment tenir compte des instructions d'utilisation et des obligations qui lui sont applicables.

La décision de lancement, ainsi que la finalité retenue, doivent enfin être formalisées dans la documentation du projet, en tenant en compte, le cas échéant, des exigences documentaires et de traçabilité applicables au titre du RIA.

IV.4 Specification des objectifs metiers

Une fois la décision de lancement du projet actée, la phase de spécification des objectifs métiers commence. Il convient alors de sélectionner soigneusement les métriques qui seront suivies tout au long du projet afin d'en assurer le pilotage.

Ces métriques se divisent en deux catégories principales :

- les **métriques orientées métier,** qui permettent de mesurer l'impact et l'efficacité du SIA au regard des objectifs commerciaux ou opérationnels de l'entreprise ;
- les **métriques orientées *data science***, qui se concentrent sur les aspects techniques et sur la performance du modèle d'IA.

Remarque : si la définition de la finalité du SIA est modifiée au cours du projet, il sera nécessaire de revenir à l'étape de « définition du projet ». Cette précaution est essentielle pour s'assurer que le projet reste aligné avec ses objectifs initiaux et, en cas de changement significatif de finalité, pour réévaluer sa pertinence et les risques associés.

Cette approche itérative permet de maintenir la cohérence du projet et de prendre pleinement en compte les conséquences d'un changement de finalité, tant sur le plan technique que sur les plan éthique et réglementaire.

RIA– Opérationnalisation

OBJECTIFS MÉTIER(1)

A cette étape, l'objectif est d'approfondir les spécifications d'un projet incluant un SIA en vue de son lancement

(1) La Phase et les Etapes font référence au livrable « *Opérationnaliser la gestion des risques* » du GT Banque du Hub France IA

HUB FRANCE IA

RIA – Opérationnalisation

OBJECTIFS MÉTIER

Boite à outils

Notre checklist pour vous aider à opérationnaliser le RIA

1. Analyse

Cadrer les besoins métiers associés au projet sélectionné avec les informations suivantes

- Expliciter les bénéfices attendus
- Déterminer la disponibilité et la qualité des données nécessaires
- Estimer la capacité à déployer la solution à la fois d'un point de vue technique et organisationnel/opérationnel

- **Liste des questions** qui organise l'expression des besoins
- **Outils et procédures** d'estimation de la valeur

❑ **Note de cadrage** d'expression des besoins
❑ **Fichier d'estimation de la valeur** du projet
❑ **Fiche projet** – Mise à jour :
- décrire la finalité ;
- affiner/confirmer/corriger le niveau de risque/criticité du projet par rapport au RIA ;
- décrire la *DATA* visée pour les différentes phases du projet (disponibilité, qualité, source…) et identifier les données personnelles.

2. Décision

Décider du lancement du projet

- Évaluer la phase précédente
- Vérifier la disponibilité des équipes techniques

- **Cadre pour** estimer la valeur apportée
- **Grille d'évaluation** de faisabilité de projet
- **Annuaire** des rôles et responsabilités pour le projet

❑ **Formalisation de la décision de lancement**
❑ **Fiche projet** – Mise à jour :
- tracer la décision prise (lancement et potentielles réserves

3. Spécification

Spécifier des objectifs métiers en sélectionnant les métriques qui seront suivies lors du projet

- Métriques orientées métier
- Métriques orientées data science

- **Liste de métriques standards** (métier et data science)
- **Outil d'archivage des métriques**
- **Outil de suivi des métriques**

❑ **Production et consignation des métriques standards**
❑ **Fiche projet** – Mise à jour :
- préciser la destination et/ou finalité ;
- Affiner/confirmer/corriger niveau de risque/criticité du projet par rapport au RIA ;
- préciser la *DATA* visée pour les différentes phases de projet (disponibilité, qualité, source, …) et identifier les données personnelles

HUB FRANCE .IA

RIA– Opérationnalisation

OBJECTIFS MÉTIER

Le Hub France IA a identifié à ce jour des éléments qui doivent être pris en compte à chacune des étapes de la phase de « objectifs métier»

A toutes les étapes

Proposition d'outils / processus d'aide à la mise en conformité

- Processus de gestion de projet de la filière métier (ex. Procédure de décision projet)
- Politiques internes de la filière métier relatives à la DATA, l'IA et l'éthique/droits fondamentaux
- Formations et référentiels de compétences liés à l'IA spécifiques à la filière métier
- Base de connaissance de la DATA et KPI nécessaires pour les projets d'IA

Notre checklist pour vous aider à opérationnaliser l'AI Act

- ❑ **Registre des décisions**
- ❑ **Preuve de formation** d'acculturation IA des salariés sur le domaine visé (Art.4, Cons.20 RIA)

HUB FRANCE IA

V. Gouvernance des données

V. GOUVERNANCE DES DONNEES

V.1 INTRODUCTION

La gouvernance des données, bien que non définie de manière autonome dans le RIA, peut être appréhendée à partir d'une lecture combinée du considérant 27 et de l'article 10 du RIA. Le Hub France IA propose de définir la gouvernance des données comme « **l'usage technique des données d'entrainement, de validation et de tests dans le respect de la réglementation, afin d'identifier, de mesurer, et de gérer les risques** ».

La gouvernance des données, telle que prévue par l'article 10 du RIA, doit **impérativement** être mise en place pour les **SIA à haut risque**. Des exigences spécifiques sont également prévues pour les **fournisseurs des modèles *GPAI*** (art. 53). Ceux-ci doivent notamment mettre en place « une **politique** visant à se conformer au droit de l'Union en matière de **droit d'auteur** et de **droit voisins** [et notamment à identifier et respecter, y compris au moyen de technologies de pointe, une réservation de droits exprimée] » (art. 53, §1, c)[11].

Par **principe**, les **exigences** prévues en matière de gouvernance des données s'appliquent aux **données d'entraînement, de validation et de test**. Par conséquent, elles doivent être prises en compte au long du cycle de vie du projet.

Par **exception à ce principe**, sont exclus les SIA qui ne font pas appel à des techniques impliquant l'entraînement de modèles d'IA. Dans ce cas, ces exigences s'appliquent uniquement aux jeux de données de test (art. 10, §6).

[11] Cette exigence de conformité au droit d'auteur fait l'objet, en France, de travaux venant en préciser la portée. Le Conseil supérieur de la propriété littéraire et artistique (CSPLA) a ainsi remis, en décembre 2024, un rapport proposant un modèle de « résumé suffisamment détaillé » des données d'entraînement (art. 53, §1, d), appelé à intégrer les mesures de respect de la réservation de droits (« opt-out ») de l'article 53, §1, c). En parallèle, la proposition de loi dite « Darcos », déposée au Sénat le 12 décembre 2025 et adoptée en première lecture le 8 avril 2026 — mais non entrée en vigueur à ce jour —, tend à instaurer une présomption réfragable d'utilisation des contenus protégés par les fournisseurs de systèmes d'IA (futur article L. 331-4-1 du code de la propriété intellectuelle), afin de renforcer l'effectivité des droits des ayants droit. Ces développements confirment que la gouvernance des données doit intégrer, dès la collecte, la traçabilité de la provenance et de la licéité des jeux d'entraînement au regard du droit d'auteur. Conseil Supérieur de la Propriété Littéraire et Artistique. Rapport de mission relative à la mise en œuvre du règlement européen établissant des règles harmonisées sur l'intelligence artificielle (« template »). 9 décembre 2024. https://www.culture.gouv.fr/mc/content/download/366050/file/CSPLA_Rapport_IA_Template_Dec_.2024.pdf?inLanguage=fre-FR&version=1
Sénat. Proposition de loi adoptée par le Sénat, relative à l'instauration d'une présomption d'utilisation des contenus culturels par les fournisseurs d'intelligence artificielle. (dite Loi « Darcos »). 9 avril 2026. https://www.assemblee-nationale.fr/dyn/17/textes/l17b2634_proposition-loi

Dans les organisations, ces exigences en matière de gouvernance des données doivent figurer à la fois dans les **politiques de gestion des risques** et dans les **politiques de gestion de la qualité**. Ces dernières doivent prévoir les règles et procédures applicables à la gestion des données lors des opérations de leurs opérations de traitement, de la collecte à la conservation.

En complément du RIA, des **normes techniques** ont été commandées par la Commission européenne aux organismes européens de normalisation **CEN-CENELEC**. Ces normes techniques ne sont pas connues publiquement à ce jour. Leur objet porte notamment sur « **la gouvernance et la qualité des jeux de données utilisées pour développer les SIA** ».

En synthèse, l'étape projet « gouvernance des données » peut s'articuler autour de trois sous-étapes principales :

1. la **collecte** des données ;
2. la **connaissance** des données ;
3. le prétraitement et l'enrichissement des données.

Chacune de ces sous-étapes comporte ses propres exigences. Pour chacune d'elles, le GT BAIA a cherché à opérationnaliser autant que possible les exigences réglementaires afin de répondre aux besoins opérationnels.

V.2 COLLECTE DES DONNEES

L'article 10 prévoit des exigences spécifiques applicables à la collecte des données, afin de contribuer à la gestion des risques. Il s'agit notamment de s'assurer de la licéité de la collecte, des éventuels consentements à obtenir, et du droit de réutilisation des données collectées.

Pour ce faire, il est essentiel de :

1. s'assurer que la collecte respecte la **réglementation applicable et les référentiels internes** prévus à cette étape ;
2. respecter le **principe de minimisation** lorsque des données à caractère personnel (DCP) sont collectées.

Il est essentiel de **documenter par écrit** l'ensemble de ces éléments afin d'alimenter la documentation technique requise (art. 11 annexe IV) et de mettre à jour la fiche

projet interne en indiquant de quelle manière les données ont été obtenue et sélectionnées.

Pour les **fournisseurs des modèles *GPAI***, des **informations** concernant la manière dont les données ont été collectées devront figurer dans le modèle de résumé à établir, notamment afin de contribuer au respect du droit d'auteur et des droits voisins (art. 53).

V.3 CONNAISSANCE DES DONNEES

A cette étape, afin de répondre aux exigences réglementaires, il est essentiel de s'assurer que les données collectées sont de **qualité**, en évaluant notamment leur disponibilité, leur quantité, et leur adéquation (art. 10, § 2).

Pour ce faire, il convient de **décrire** les **jeux de données**, de les **insérer** dans **un catalogue ou un dictionnaire de données** et de **documenter** de manière détaillée ces opérations. La réglementation demande expressément de documenter les informations relatives à la provenance, à la portée et aux principales caractéristiques des données (Art. 11, Annexe IV).

En particulier :

- vérifier la pertinence, la représentativité, l'absence d'erreur et de données manquantes, ainsi que la présence éventuelle de biais ;
- indiquer les caractéristiques des données collectées ;
- prendre en compte le **contexte géographique, contextuel, comportemental ou fonctionnel**, dans lesquels les SIA sont destinés à être utilisés (art. 10 §4, et 42).

D'un point de vue opérationnel, des contrôles doivent être mis en place afin de s'assurer que **les données collectées** sont **conformes aux attentes techniques** :

- **format des données** : vérifier que les types de données (par exemple, entier, nombre flottant, chaîne de caractères, etc.) et les noms des colonnes sont conformes à l'expression de besoins. Pour les données textuelles, vérifier qu'elles sont décodables sans caractères corrompus (par exemple, encodage UTF-8). Pour les images et les vidéos, vérifier le format (JPEG, PNG, MP4, AVI, etc.) et la résolution minimale (en pixels). Vérifier également les formats spécifiques aux données (par exemple, code pays ISO, numéros de téléphone, dates, etc.). Pour les données textuelles, détecter les erreurs d'extractions (par exemple, erreurs

d'OCR[12]) et de conversion (par exemple, conversion de PDF, HTML ou XML). Vérifier également que les données textuelles sont dans la langue attendue ;
- **cohérence des données** : contrôler le volume de données et sa cohérence avec l'historique sur le périmètre d'application ;
- **qualité des données** : identifier et traiter les doublons (par exemple, unicité des identifiants). Vérifier la complétude à la source en s'assurant que les champs obligatoires sont présents et contrôler la fraîcheur des données en vérifiant leurs dates de mise à jour. Documenter la provenance (*data lineage*) en identifiant le système source, la date d'extraction et la version des données.

Après avoir vérifié le format, la cohérence et la qualité des données, le *data scientist* doit analyser, lors de la phase d'exploration et d'analyse des données :

- **le profil statistique** des données : analyser les distributions à l'aide d'outils tels que les *box plots*, calculer les moyennes, les médianes et les écarts-types pour les variables continues, les modes pour les variables catégorielles et la fréquence des termes pour les données textuelles ;
- **les valeurs manquantes** : calculer les taux de valeurs manquantes par variable et vérifier si ces valeurs sont aléatoires ou informatives. Pour les données textuelles, identifier les textes vides ou tronqués (par exemple, minimum et maximum du nombre de *tokens*) ;
- **les anomalies** : détecter les anomalies à l'aide des outils tels que l'*Interquartile Range* (IQR), les *z-scores* ou des modèles de *machine learning* de détection d'anomalies (par exemple, *Isolation Forest*). Pour les données textuelles, mesurer le taux de mots hors vocabulaire et identifier les fautes d'orthographe récurrentes ;
- **l'analyse des données :** analyser les modalités des variables catégorielles, c'est-à-dire le nombre de valeurs distinctes ;
- **les dérives statistiques :** analyser les potentielles dérives de distribution en calculant des indicateurs adaptés, tels que le *Population Stability Index ou,* selon le besoin, des mesures de divergence entre distributions (par exemple, la divergence de *Kullback-Leibler symétrisée*) ;

[12] *Optical character recognition.*

- **les corrélations** : analyser les corrélations entre les variables et les potentiels problèmes de multicolinéarité à l'aide, notamment, du *Variance Inflation Factor* (*VIF*) ;
- **la *target distribution*** : dans les modèles supervisés, vérifier la distribution de la variable cible, pour documenter, si nécessaire, les stratégies de rééquilibrage ;
- **les images et vidéos :** pour les images, analyser la netteté, la luminosité et le contraste, ainsi que le nombre de canaux (un pour le noir et blanc, trois pour le *RGB*). D'autres contrôles peuvent être appliqués aux vidéos, notamment la qualité de la compression, la synchronisation entre les pistes audio et vidéo, la présence de séquences d'écrans noirs ou d'images figées et le nombre d'images par seconde.

V.4 PRETRAITEMENT ET ENRICHISSEMENT DES DONNEES

Pendant cette phase, il convient d'effectuer les **opérations de recodage** et **d'enrichissement** nécessaires au traitement attendu.

Ces opérations doivent être **documentées et décrites de manière détaillée**. Il s'agit, à cette étape, de :

- nettoyer, annoter, extraire des caractéristiques et répartir des données (prétraitement) ;
- détecter, prévenir et atténuer les éventuels biais (Art. 10, §2, g) ;
- le cas échéant, enrichir les données.

D'un point de vue opérationnel, lors de la phase de préparation et de transformation des données, le *data scientist* doit notamment vérifier :

- **le traitement de valeurs manquantes** : contrôler validité de la méthode d'imputation retenue (par exemple, moyenne, médiane, mode, valeur conservatrice, ou utilisation d'un modèle de *machine learning* tel que *KNN*[13]) et mesurer son impact ;
- **l'encodage :** vérifier la pertinence de l'encodage des variables (*label encoding* ou *one-hot encoding* pour les variables catégorielles) et identifier les catégories rares ;

[13] *K-Nearest Neighbors.*

- **les transformations des variables :** normalisation, standardisation ou transformation de variables continues en variables catégorielles (*binning*) ;
- **l'intégrité :** contrôler l'intégrité et le maintien de l'exhaustivité de la base lors des jointures de différentes tables, en identifiant de potentielles pertes de lignes ou d'observations ;
- ***le Target Leakage*** : s'assurer de l'absence de fuite de données dans les variables utilisées pour le modèle. On peut notamment citer deux exemples de fuite de données : l'utilisation d'un *proxy* de la variable cible comme variable explicative ou l'utilisation d'une variable reposant sur une information qui ne serait pas disponible au moment de la prédiction ;
- **les biais :** contrôler la présence potentielle de biais en comparant la distribution de la variable cible entre les populations à risque préalablement identifiées[14] et le reste de la population ;
- **l'anonymisation :** pour les données textuelles, détecter et masquer les données à caractère personnel en les remplaçants par des balises ;
- **la tokenisation** : contrôler la qualité de la tokenisation, notamment le taux de *tokens* hors vocabulaire ;
- le contrôle des **labels et des annotations** : vérifier la cohérence des annotations, notamment à l'aide de mesures permettant d'évaluer l'accord entre plusieurs annotateurs (par exemple, le coefficient *Kappa de Cohen)*, recourir, lorsque cela est pertinent, à l'*active learning* pour aiguiller les instances avec les labels les plus incertains. Enfin pour les images, vérifier la validité des *bounding boxes*.

Lors de la phase de découpage en échantillon d'apprentissage, de validation et de test, le *data scientist* doit notamment vérifier :

- **la représentativité :** contrôler la représentativité des distributions des classes dans les échantillons d'apprentissage, de validation et de test, en utilisant, lorsque cela est pertinent, des échantillons stratifiés ;
- **la reproductibilité** : s'assurer de la reproductibilité de la construction des jeux de données en fixant les graines des générateurs de nombres aléatoires et en documentant les paramètres utilisés ;

[14] European Union Agency for Fundamental Rights. Charte des droits fondamentaux de l'Union européenne | Article 21 - Non-discrimination |. Journal officiel de l'Union européenne C 303/17. 14 décembre 2007. https://fra.europa.eu/fr/eu-charter/charter/article/21-non-discrimination

- **la séparation** : vérifier l'indépendance des échantillons (par exemple, aucun identifiant ne doit être présent simultanément dans les échantillons d'apprentissage et de test lorsque cela compromet leur indépendance) ;
- **la temporalité** : dans le cadre des séries temporelles, contrôler que l'échantillon de test est bien postérieur à celui d'entraînement.

RIA- Opérationnalisation

GOUVERNANCE DES DONNÉES (1)

Usage technique des données dans le respect de la réglementation, afin d'identifier, de mesurer et de gérer les risques.

Étape 1 ***Collecte*** **des données** → **S'assurer que la collecte est licite , des éventuels consentements et du droit de réutilisation**

Étape 2 ***Connaissance*** **des données** → **Décrire des données, les insérer dans un catalogue, documenter, *etc*.**

Étape 3 ***Prétraitement et enrichissement*** **des données** → **Effectuer les opérations de mise en qualité nécessaires au traitement attendu**

(1) La phase et les étapes font référence au livrable « Opérationnaliser la gestion des risques » du GT Banque du Hub France IA

HUB FRANCE .IA

RIA – Opérationnalisation

GOUVERNANCE DES DONNÉES

- Cette exigence est prévue pour les **systèmes d'IA à haut risque** (art. 10) ;
- Par principe, elle concerne les **données d'entraînement, de validation et de test**. Par exception à ce principe, sont exclus les SIA qui ne font pas appel à des techniques qui impliquent l'entraînement de modèles d'IA. Dans ce cas, cette exigence s'applique uniquement aux jeux de données de test (art. 10, §6) ;
- Des **exigences spécifiques** sont aussi prévues **pour les fournisseurs de modèles de *GPAI*** : résumé synthétique des données, protection des données à caractère personnel et respect du droit d'auteur et des droits voisins (art 53, c et d) ;
- Le **système de gestion de la qualité** (art. 17) et le **système de gestion des risques** (art. 9) doivent contribuer au respect de ces exigences. La gouvernance des données doit permettre d'identifier, gérer les risques pour la santé, la sécurité et les droits fondamentaux.

Préalables nécessaires	Boite à outils	Notre *check-list* pour vous aider à opérationnaliser le RIA
Définition d'un projet et des objectifs métier	• **Questionnaire de pré analyse** des risques du SIA[2]	❑ **Analyse du niveau de risque du SIA**, et qualification du rôle de votre organisation - **Fiche projet** [2] ;
Mise en place d'un système de gestion des SIA à haut risque (art. 9)	• **Certification LNE « processus pour l'IA »** • « Cadre de gestion des risques en Intelligence Artificielle » du NIST (en attendant les normes harmonisées)	❑ **Politiques de gestion des risques à élaborer, et à mettre à jour** (art. 9) ;
Mise en place d'un système de gestion de la qualité des SIA à haut risque pour les fournisseurs (art. 17)	• **Norme ISO/IEC 42001:2023** « Système de management de l'intelligence artificielle » (en attendant les normes harmonisées)	❑ **Politiques, procédures et instructions écrites** concernant les systèmes et procédures de gestion des données (art. 17, §1, f) lors de l'acquisition, la collecte, l'analyse, l'étiquetage, le stockage, la filtration, l'exploration, l'agrégation, la conservation des données, et toute autre opération concernant les données, qui est effectuée avant la mise sur le marché, ou la mise en service, de systèmes d'IA à haut risque. .

L'analyse du HFIA préconise d'adopter la même approche pour la mise en place d'une politique de gestion de la qualité pour les fournisseurs des modèles GPAI.

[1] [2] Cf. le livrable « définition d'un projet » et « objectifs métier ». L'explication plus détaillée de la Fiche Projet est disponible dans les « concepts clés » livrés par le GT BAIA.

HUB FRANCE IA

RIA - Opérationnalisation

GOUVERNANCE DES DONNÉES

1. *Collecte* des données

Gérer les risques
- Assurer que la collecte respecte la réglementation et les référentiels internes
- **Si données à caractère personnel (DCP), respecter le principe de minimisation**

2. *Connaissance* des données

Évaluer la disponibilité, la quantité et l'adéquation de jeux de données (qualité) (art. 10, §2)
- **vérifier la pertinence, la représentativité, l'absence d'erreur et des données manquantes, la présence de biais**
- Indiquer les caractéristiques des données collectées
- Les données doivent prendre en compte le cadre géographique, contextuel, comportemental ou fonctionnel (art. 10 §4 + art. 42)

3. *Prétraitement* et *enrichissement* des données

- **Nettoyer, annoter, extraire des caractéristiques, répartir des données**
- **Détecter, prévenir et atténuer les éventuels biais**
- Si pertinent, enrichir les données

Boite à outils

- ***Check-list* des principes de collecte des données** (art. 10, § 2, b)
- ***Template* de formulaire d'accès et d'accréditation**
- **Outils de traçabilité des données (*data lineage*)**
- **Registre de traitement** si DCP
- **Modèle de résumé** prévu pour les modèles *GPAI* (art. 53, 1, d)
- **Outils d'anonymisation/pseudonymisation et/ou données synthétiques**

- **Dictionnaire et/ou catalogue de données**
- **Méthodologie de contrôle de données (qualité)**

- **Guide de bonnes pratiques** (ou même une procédure dans certains cas réglementaires)
- **Outils d'annotation, étiquetage**
- **Outils de détection et suivi des biais**
- **Outils d'anonymisation/pseudonymisation**
- **Données agrégées** et/ou **données synthétiques**
- **Feature store**
- Cadre d'utilisation du **feature store**
- **Tag des données synthétiques** pour les modèles *GPAI*

Notre *check-list* pour vous aider à opérationnaliser le RIA[3]

❑ **Fiches** avec indication de la manière dont les données ont été **obtenues et sélectionnées** (art. 11, annexe IV, § 2) ;

❑ Des informations détaillées sur la surveillance et le fonctionnement du système d'IA, en particulier en ce qui concerne (…) les spécifications concernant les **données d'entrée** (art. 11, annexe IV, § 3) ;

❑ **Résumé pour le modèle *GPAI*** (art. 53).

❑ **Fiches** sur les jeux de données (d'entraînement, validation, test) utilisés :
- Description générale de ces jeux de données ;
- Information sur leur provenance, leur portée, et leurs principales caractéristiques. (art. 11, annexe IV, § 2) ;

❑ **Notice d'utilisation** (art. 13 §3, Vi) spécifications relatives aux données d'entrée, information pertinente concernant les jeux de données d'entraînement, de validation et de test utilisés.

❑ **Fiches** sur les jeux de données (d'entraînement, validation, test) utilisés, présentant le processus de prétraitement (art. 11, annexe IV, § 2) ;

❑ **Description détaillée** sur :
- Les procédures d'étiquetage ;
- Les méthodes de nettoyage ;
- Les mentions des approches d'enrichissement de la donnée (art 10, §2, c et annexe IV).

(3) Ces livrables font partie de la documentation technique, attendue dans le cadre du RIA

LES DONNÉES DANS LE RIA

Définition RIA – Article 3

29) « **données d'entraînement** » : les donnés utilisées pour entraîner un SIA en ajustant ses paramètres entraînables ;

30) « **données de validation** » : les données utilisées pour fournir une évaluation du SIA entraîné et pour régler ses paramètres non entraînables ainsi que son processus d'apprentissage, afin, notamment, d'éviter tout sous-ajustement ou surajustement ;

31) « **jeu de données de validation** » : un jeu de données distinct ou une partie du jeu de données d'entraînement, sous la forme d'une division variable ou fixe ;

32) « **données de test** » : les données utilisées pour fournir une évaluation indépendante du SIA afin de confirmer la performance attendue de ce système avant sa mise sur le marché ou sa mise en service ;

33) « **données d'entrée** » (*inputs*), : les données fournies à un SIA ou directement acquises par celui-ci et à partir desquelles il produit une sortie ;

34) « **données biométriques**» : v. définitions clés.

Proposition de contenu

Tout d'abord, le « jeu de données » n'est pas définit dans le RIA. Il s'agit d'un ensemble de données utilisées, soit pour produire un SIA, soit pour l'utiliser.

Les différentes définitions fournies par l'article 3 concernant les données reprennent le langage technique typique de l'apprentissage automatique/machine (*Machime Learning* ou *ML*). Ces définitions peuvent peuvent avoir une acception plus large dans la pratique que dans le texte, et doivent donc être interprétées avec précaution.

Pour simplifier, on peut imaginer la calibration classique d'un modèle d'apprentissage automatique/machine en 3 étapes :

- **apprentissage :** le système s'entraîne sur ces données pour effectuer la tâche attendue ; à cette étape, il s'agit des données **d'entraînement** (29) ;
- **validation** : estimation de l'erreur de prédiction pour la sélection du modèle et l'optimisation des hyperparamètres ; à cette étape, il s'agit des données **de validation** (30) ;
- **test** : évaluation de l'erreur de généralisation du modèle final choisi ; à cette étape, il s'agit des données **de test** (32).

Il est important de respecter les spécificités de chaque jeu de données à chaque étape, à défaut, d'entraîner une surestimation des performances du modèle.

Les **données d'entrée** sont des données utilisées pour la prise de décision du SIA en production. Elles ne sont pas spécifiquement mentionnées par le RIA à l'article 10. Toutefois, le Hub France IA considère que les mêmes exigences en termes de qualité devraient être également garanties pour ces données.

Les **données synthétiques** sont des données générées artificiellement dont l'objectif est d'imiter et simuler les caractéristiques de l'ensemble de données d'origine. Il existe différentes méthodes pour générer des données synthétiques (extraction, reproduction des propriétés des données d'origine, utilisation de connaissances d'experts, ou de processus connus). Les données synthétiques présentent l'avantage considérable de bénéficier d'un régime juridique allégé, ce qui facilite l'utilisation par rapport à des données réelles.

HUB FRANCE IA

VI. Classification RIA : scenarii de classification

VI. CLASSIFICATION RIA : SCENARRII DE CLASSIFICATION

VI.1 Introduction

Le RIA repose sur une **approche fondée sur les risques**, visant à adapter les obligations juridiques applicables aux acteurs en fonction du niveau du risque que présente un SIA pour les droits fondamentaux, la sécurité ou la santé. Cette approche ne se limite toutefois pas à une classification pyramidale. Elle introduit une logique dans laquelle un même système peut être soumis à **plusieurs catégories d'obligations cumulatives**.

Le règlement prévoit tout d'abord plusieurs exclusions, totales ou partielles, de son champ d'application, notamment pour certains systèmes utilisés à des fins militaires, de défense ou de sécurité nationale (cons. 24), à des fins de recherche scientifique et de développement (cons. 25), pour un usage exclusivement personnel (cons. 25), ou encore pour certains modèles ou systèmes distribués sous des licences libres et ouvertes, dans les conditions prévues par le règlement (cons. 89).

Pour les systèmes relevant du champ d'application du règlement, **quatre niveaux de risque** sont prévus :

1. risque inacceptable ;
2. haut risque ;
3. système avec obligations de transparence ;
4. système sans obligation spécifique (risque minimal).

Cependant, les **obligations** applicables ne dépendent pas uniquement du niveau de risque. Elles peuvent également varier en fonction du rôle de l'acteur concerné (fournisseur, déployeur, importateur, distributeur, *etc.*) de la nature du système et de sa structure technique.

Ainsi, un même SIA peut, par exemple, relever de la catégorie des SIA à haut risque, intégrer un modèle à usage général, et être également soumis à des obligations spécifiques de transparence. Le règlement ne prévoit **pas nécessairement d'exclusion automatique entre ces différentes catégories**, ce qui impose d'identifier et d'analyser leur éventuel cumul.

Pour faciliter la compréhension de cette logique, huit scénarios types ont été identifiés afin d'illustrer les principales combinaisons possibles d'obligations réglementaires. Ces scénarios permettent de comprendre concrètement comment se déterminent les obligations applicables en fonction des caractéristiques du système, de son utilisation et des choix techniques et commerciaux opérés autour de celui-ci.

RIA: différents scénarii de classification

Les exigences prescrites par le règlement pour un système d'IA varient selon que le système d'IA appartient à l'une ou à plusieurs des catégories suivantes :

- **SIA à Haut Risque** ;
- **SIA intégrant un GPAIm** (à risque systémique ou pas) ;
- **SIA avec obligations particuliers de transparence** ;

Pour chacune de ces catégories, le règlement définit des exigences et des actions spécifiques qui doivent être définies, réalisées et documentées au cours du processus de modélisation.

Ces catégories **ne s'excluent pas mutuellement**, ce qui signifie qu'un système peut potentiellement répondre aux exigences de ces trois catégories. Après avoir défini cette structure, il est possible d'identifier 8 cas possibles présentés ci-dessous.

Avertissement: les systèmes présentés sont utilisés à titre d'exemple pour la catégorie. Cela ne signifie pas que ces systèmes sont développés ou qu'ils devraient l'être. Les combinaisons avec des systèmes interdits sont exclues de cette discussion car elles ne peuvent pas être utilisées.

RIA : différents scénarii de classification

SIA à risque minime : SIA pour les recommandations de musiques ou livres.

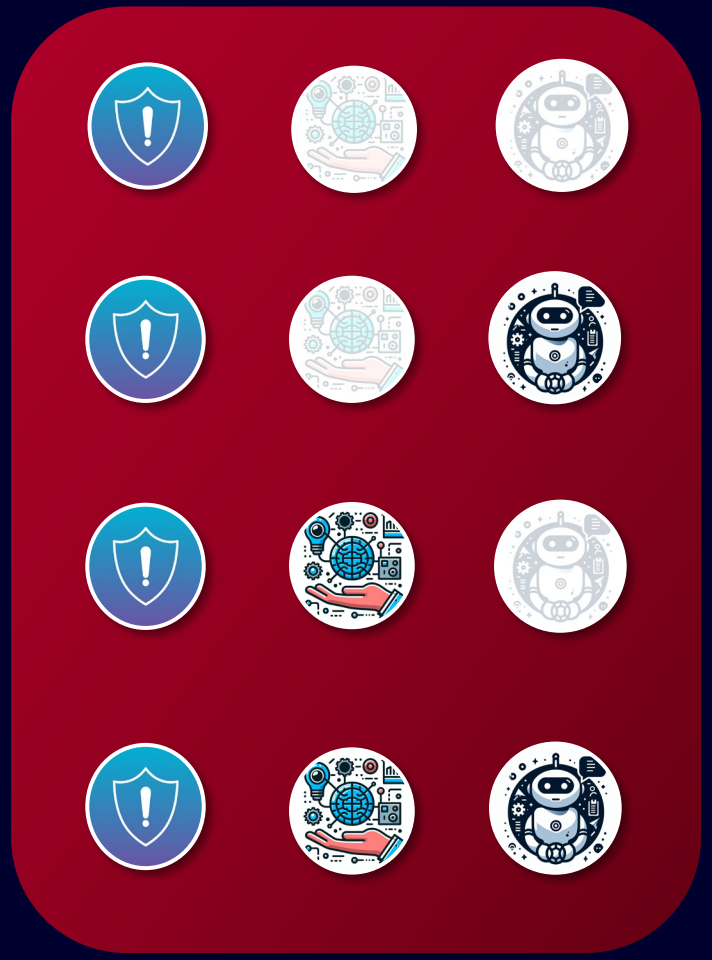
Chatbot avec des questions prédéfinies (pas d'IA générative). *Chatbot FAQ* p.ex. navigation site web).

Système *GPAI* générant du contenu fidèle aux données d'entrée ou revue par un humain, non appliqué à un cas d'usage à haut risque : Modèle utilisé pour générer une traduction ou pour transcrire la voix via *LLM*.

Système GPAI générant du contenu ou interagissant avec un utilisateur, non appliqué à un cas d'usage à haut risque : *Chat GPT*.

Considérations RIA Classification

Haut Risque	*GPAI*	Transparence



<u>SIA à haut risque</u> : Système d'IA d'octroi de crédit aux particuliers.

<u>Chatbot avec des questions prédéfinies</u> <u>(pas d'IA générative)</u>**<u>, utilisé pour un usage à haut risque</u>** : Modèle d'octroi basé sur un arbre de décision, accessible par les consommateurs individuels via un chatbot (pour saisir les informations de crédit requises).

<u>Système GPAI fidèle aux données d'entrée ou revue par un humain appliqué à un cas d'usage à haut risque</u> : Système intégrant un modèle *GPAI* qui propose des formations à partir d'un catalogue, sur la base d'une évaluation des besoins et des acquis.

<u>Système *GPAI*, générant du contenu ou interagissant avec un utilisateur, appliqué à un cas d'usage à haut risque</u> : Système à destination des RH pour tri et sélection des CV pour une proposition d'entretiens

HUB FRANCE IA

VII. Modélisation

VII. MODELISATION

VII.1 Introduction

La phase de modélisation constitue une étape clé dans tout développement d'un SIA. L'objectif est de développer, évaluer et sélectionner un SIA en garantissant sa cohérence technique, sa qualité, sa robustesse et sa conformité réglementaire.

Cette phase inclut généralement des bonnes pratiques relatives à la qualité des données, à la solidité conceptuelle du système, à l'évaluation correcte des performances et de ses limites, à sa sécurisation technique ainsi qu'à la mise en place d'un cadre de suivi continu.

Pour chacun de ces axes, une entreprise devrait disposer de procédures et de lignes directrices permettant aux équipes chargées de la modélisation de s'aligner sur les normes et les attentes applicables. Ce document met principalement l'accent sur les exigences découlant du RIA. Les bonnes pratiques générales de modélisation ne seront donc pas abordées plus en détail dans ce livret blanc. Pour plus d'informations sur les bonnes pratiques et la gestion des risques lors de l'étape de modélisation on vous invite à faire référence au Livre blanc du GT Banque[15].

Conformément à la structure définie dans le Livre blanc du GT Banque, la phase de modélisation est organisée en trois sous-phases :

1. **construction du modèle :** développer un SIA en suivant une méthodologie standardisée afin d'assurer sa cohérence et sa qualité ;
2. **évaluation du modèle :** évaluer les performances du modèle au regard des objectifs définis, de références pertinentes et, lorsque cela est approprié, de processus existant ou des performances humaines ;
3. **sélection du modèle :** choisir le modèle présentant le profil le plus adapté vis-à-vis des critères relatifs aux exigences techniques, réglementaires et métier, en

[15] Hub France IA. Livre blanc : Contrôle des risques des systèmes d'Intelligence Artificielle. Octobre 2022. https://www.hub-franceia.fr/wp-content/uploads/2022/10/22_10_19_Controle-des-risques-des-systemes-IA_PDF.pdf et Hub France IA. Livre blanc : Opérationnaliser la gestion des risques des systèmes d'intelligence artificielle. Juillet 2024. https://www.hub-franceia.fr/wp-content/uploads/2024/07/Hub-France-IA-Operationnaliser-la-gestion-des-risques.pdf

tenant notamment compte de l'interprétabilité, les biais, des performances et des contraintes opérationnelles avant sa validation finale.

Avant d'engager cette phase, il est essentiel pour l'organisation de vérifier l'existence et l'applicabilité des **normes internes transverses**, tout en identifiant les **exigences réglementaires spécifiques** au projet.

Ces référentiels peuvent notamment inclure des politiques de gestion des risques, des modèles standardisés de documentation ainsi que des procédures dédiées à la gestion des risques *IT*. Dans les organisations complexes, les politiques encadrant la conception, l'évaluation et la sélection des modèles jouent également un rôle déterminant. Elles permettent d'harmoniser les pratiques de développement, de renforcer la robustesse des solutions et de faciliter leur validation ainsi que leur suivi dans la durée.

Comme rappelé dans la section VI, les exigences sont définies selon des axes de risque et sont cumulatives. Pour cette raison, il a été jugé pertinent de présenter les exigences du RIA en les structurant par axes, notamment les SIA à haut risque dans la section VII.2 et les modèles *GPAI* dans la section VII.3.

Les exigences spécifiques relatives à la transparence ne font pas l'objet d'un développement particulier dans cette partie consacrée à la modélisation. Les sections VII.5 et VII.6 présentent une structuration possible de deux documents clés : respectivement la « Documentation du modèle » et la « Notice d'utilisation ».

VII.2 Modelisation – Focus Haut Risque

Les SIA classés à haut risque sont soumis aux exigences de conformité les plus strictes du RIA. La phase de modélisation constitue, à ce titre, une étape déterminante, au cours de laquelle la majorité des contrôles et mesures requis doivent être réalisés, démontrés et documentés.

Les exigences principales afférentes à la construction d'un modèle estampillé haut risque sont les suivantes :

- **structurer la gestion des risques (art. 9) :** assurer l'alignement du projet avec le système de gestion des risques de l'entreprise et mettre en place un processus itératif permettant d'identifier, d'analyser, d'évaluer et de traiter les risques. Il

convient également d'amorcer la définition d'un dispositif de journalisation conforme à l'article 12. Celui-ci doit permettre identifier les situations potentiellement à risque, de tracer les modifications substantielles et de suivre les principaux indicateurs de performance. Des exigences spécifiques s'appliquent aux SIA visés à l'annexe III, point 1.a ;

- **préparer les données nécessaires à la modélisation (art. 10) :** sélectionner, prétraiter et enrichir les jeux de données selon les orientations définies lors de la gouvernance des données. Des ajustements finaux (normalisation, encodage, agrégation, *etc.*) sont réalisés au moment de la modélisation, car ils dépendent notamment du type d'algorithme choisi. Un modèle fondé sur la minimisation de distances n'exige ainsi pas nécessairement les mêmes traitements qu'un modèle à base d'arbres. Cette étape achève donc le travail amorcé lors de la phase précédente ;
- **concevoir les mécanismes de supervision humaine (art. 14) :** initier la conception d'un dispositif permettant à des personnes physiques de superviser et, le cas échéant, de contrôler le fonctionnement du SIA. Les modalités de supervision doivent être proportionnées au niveau de risque du système et adaptées à son contexte d'utilisation ;
- **définir les exigences de performance et de résilience (art. 15) :** concevoir un système capable d'atteindre un niveau approprié de précision, de robustesse et de cybersécurité, en s'appuyant sur des référentiels, des critères d'évaluation et des méthodes de mesure adaptés. Ces exigences doivent rester cohérentes avec les objectifs définis dans la fiche projet ainsi qu'avec les éventuels seuils de performance fixés par les normes internes de modélisation et les réglementations sectorielles ou spécifiques, en complément des exigences identifiées par le RIA.

  Le choix des métriques doit être adapté au cas d'usage et tenir compte notamment du périmètre d'application, du déséquilibre éventuel des classes et de l'évolution dans le temps du phénomène modélisé. La nature et la complexité du modèle retenu peuvent par ailleurs justifier des niveaux de validation et de preuve de conformité plus ou moins approfondis.

  Les exigences de résilience doivent ainsi être définies selon une approche fondée sur les risques et proportionnées au niveau de risque du SIA. Cette analyse doit notamment prendre en considération le profil des utilisateurs ayant accès au système (collaborateurs, clients ou grand public), la présence éventuelle de données sensibles ainsi que les dépendances à des applications ou services

tiers intégrés au processus. Des précisions supplémentaires à ce sujet devraient être fournies par les normes harmonisées ;

- **actualiser la documentation technique (art. 11) :** mettre à jour la documentation technique du SIA conformément aux exigences prévues à l'annexe IV, afin de refléter les choix de conception, les caractéristiques du système et les mesures de maîtrise mises en œuvre. Les éléments attendus dans ce document sont présentés dans la section VII.5 ;
- **élaborer la notice d'utilisation (art. 13) :** rédiger une notice claire et complète à destination des déployeurs, précisant notamment les conditions d'utilisation du système, ses capacités, ses limites, les modalités de supervision humaine et les précautions à respecter. Les éléments attendus dans ce document sont présentés dans la section VII.6.

Lors de la **phase d'évaluation du modèle**, l'objectif est de d'itérer jusqu'à atteindre les performances attendues dans le respect des contraintes fonctionnelles, techniques et réglementaires applicables. Il s'agit donc de construire, avec les différentes parties prenantes, un **protocole d'évaluation,** puis de l'exécuter.

Cette démarche peut s'appuyer sur des outils de *benchmarking*, de détection des biais, ainsi que sur des dispositifs d'interface homme-machine et de supervision humaine permettant d'évaluer les conditions réelles d'utilisation et de contrôle du système.

Enfin, la sélection du modèle destiné à être déployé en production doit être structurée. Il est ainsi recommandé de **construire et d'utiliser,** avec les différentes parties prenantes, **un protocole de sélection de modèle.** Celui-ci pourrait notamment s'appuyer sur les **outils** suivants :

- métriques métiers et *data science ;*
- outils d'explicabilité et quantification d'incertitude.

VII.3 Modelisation – Focus modeles *GPAI*

Lors de la construction **d'un modèle *GPAI*** (art. 53), les obligations incombant aux fournisseurs, et étendues aux entreprises qui *fine-tune* un modèle *GPAI*, exclusivement sur les parties modifiées/ nouvellement introduites (cons. 109), sont :

- établir et tenir à jour la documentation technique du modèle ;

- élaborer, tenir à jour et mettre à disposition la documentation permettant de bien comprendre **les capacités et les limites du modèle *GPAI*** ;
- mettre en place une politique visant à respecter le droit de l'Union, notamment en matière de droit d'auteur et de droits voisins ;
- établir et mettre à disposition un résumé suffisamment détaillé de la donnée utilisé pour l'entraînement du modèle *GPAI*.

Certaines interventions en aval, notamment le *fine-tuning*, peuvent conduire l'acteur à être soumis à des obligations comparables à celles du fournisseur du modèle *GPAI*, dans les conditions prévues par le RIA, mais uniquement pour les éléments modifiés ou nouvellement introduits (considérant 109).

Cette responsabilité s'applique lorsque l**a modification entraîne un changement important de la généralité, des capacités ou du risque systémique du modèle**. Le critère établi pour satisfaire à cette condition est d'avoir utilisé, pour cette modification, une **puissance de calcul supérieure à un tiers de celle utilisée pour l'entraînement du modèle original**.

En l'absence d'informations fiables sur la puissance de calcul mobilisée pour l'entraînement du modèle initial, le seuil de 10^{23} opérations peut être retenu comme valeur de référence.

Les obligations énoncées ne s'appliquent pas aux modèles d'IA qui sont publiés en licence libre et ouverte sauf s'ils présentent un risque systémique (Art. 53.2).

Les outils préconisés afin de faciliter l'opérationnalisation de ces obligations sont :

- un *standard* de construction du modèle ;
- un *template* de documentation du modèle ;
- un modèle de résumé des données d'entrainement du modèle *GPAI* fourni par le Bureau de l'IA ;
- un *template* de la déclaration de respect des lois européennes sur les droits d'auteur.

Lors de l'évaluation du modèle, deux exigences sont à suivre.

Tout d'abord il s'agit de **classifier** des systèmes présentant **un risque systémique** (art. 51), ensuite d'**informer** la Commission et/ou présenter les éléments pour demander une exemption (si applicable – art. 52). Ensuite, il faut fournir une évaluation du modèle et une piste d'audit des tests.

RIA – Opérationnalisation

MODÉLISATION (1)

Guider l'alignement entre les bonnes pratiques du processus de modélisation et les exigences du RIA, qui dépendent de la qualification du Système d'IA en cours de réalisation. Le niveau de détail et les exigences décrits dans ce livrable seront étroitement liés avec les spécifications des normes harmonisées à paraître dans le cadre du RIA.

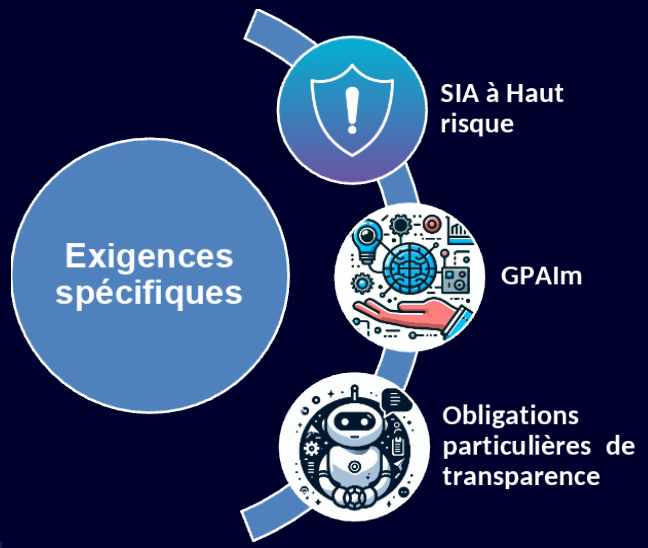
Étape 1 **Construction du modèle**	**Développer un système d'IA en suivant une méthodologie standardisée pour assurer cohérence et qualité.**
Étape 2 **Évaluation du modèle**	**Comparer les performances du modèle avec des processus existants ou des références humaines.**
Étape 3 **Sélection du modèle**	**Choisir le modèle présentant le profil le plus adapté vis à vis de critères relatifs aux exigences techniques, réglementaires et métier, en tenant compte de l'interprétabilité, les biais et les contraintes opérationnelles avant validation finale.**

(1) La phase et les étapes font référence au livrable « Opérationnaliser la gestion des risques » du *GT Banque* du Hub France IA.

HUB FRANCE .IA

RIA – Opérationnalisation

MODÉLISATION



Les exigences et actions attendues par le RIA au cours du processus de modélisation varient en fonction du type de système d'IA : **SIA à haut risque**, **SIA à usage général** (systémique ou pas), **SIA avec obligations particuliers de transparence**.

- Ces catégories ne s'excluent pas mutuellement; un système peut donc potentiellement répondre aux exigences de ces trois catégories (cf. feuillet *RIA différents scénarii de classification*).
- Pour plus d'informations sur le processus de modélisation, nous vous recommandons de consulter les lignes directrices élaborées par le *GT Banque*.

Préalables nécessaires

Normes internes transversales et réglementations spécifiques

Documents associés au projet (phases préalables)

Boîte à outils

- **Standards NIST** : Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations
- **MITRE ATLAS** - Base de tactiques et de techniques adverses contre les systèmes basés sur l'IA.
- **HELM** : *reproducible and transparent framework for evaluating foundation models*
- **OWASP** : *LLM & Generative AI Security Risk*
- **ANSSI** : Développer la confiance dans l'IA par une approche par les risques cyber. 7 février 2025
- **OECD:** Toolbox Trustworthy AI
- **À paraître** : Normes harmonisées validées par la Commission EU.

Notre check-list pour vous aider à opérationnaliser le RIA

- ❑ Les **réglementations spécifiques** à un domaine qui doivent être respectées en complément des exigences identifiées par le RIA.
- ❑ **Politiques de gestion de risques** à élaborer, et à mettre à jour (Art. 9).
- ❑ **Politiques de construction, évaluation,** (dont protocole de Stress Test), **sélection du modèle,** y compris modèles *GPAI* (Système de gestion de qualité - Art. 17 point b./c./d.)
- ❑ **Template documentation modèle** (Art. 11).
- ❑ **Politiques de gestion du risque IT** : mesures visant à assurer la **robustesse, la résilience et la cybersécurité** des systèmes (Art. 15).

- ❑ **Fiche projet,** transversale à toutes les étapes du projet et essentielle pour déterminer la diligence en matière de modélisation en fonction de la classification RIA du cas d'utilisation proposé.
- ❑ **Documentation technique** contenant les informations sur les données (train/validation/test), le processus de collecte et le prétraitement appliqué.

(1) L'explication plus détaillée de la Fiche Projet est disponible dans les définitions clés livrées par le GT BAIA.

HUB FRANCE IA

RIA – Opérationnalisation

MODÉLISATION - FOCUS HAUT RISQUE

1. Construction du modèle

- **Gérer les risques.** Assurer l'alignement avec le système de gestion des risques de l'entreprise (Art. 9) et commencer à définir un système de log (Art. 12) capable d'identifier les situations potentiellement à risque, les modifications substantielles, les KPI de suivi (spécificités pour SIA visés à l'Annexe III, point 1.a).
- Dans le cadre du design du modèle, **sélectionner, prétraiter et enrichir les données** Focus sur les traitements de données propres à l'étape de modélisation (cf. Phase de gouvernance des données).
- **Mettre à jour la documentation technique (Annexe IV).**
- **Production de la notice d'utilisation** à destination des déployeurs.
- **Initier la conception d'un système permettant le contrôle du SIA par des personnes physiques,** en fonction du niveau de risque associé au SIA et de son cadre d'application (Art. 14).
- **Élaborer un système résilient** visant à atteindre un niveau approprié de précision, de robustesse et de cybersécurité, en s'appuyant sur des critères de référence et des méthodes de mesure appropriées (Art. 15, en attente des normes harmonisées).

Boîte à outils

- Système de gestion des risques
- Standard de construction des modèles candidats (stratégies d'apprentissage, architecture, familles de modèles compatibles avec les contraintes/obligations, etc)
- Template de documentation du modèle
- Template de construction de pipeline
- Outils de versioning
- Les réglementations sectorielles et/ou spécifiques en complément des exigences identifiées par le RIA.

2. Évaluation du modèle

Itérer jusqu'à converger vers les exigences attendues dans le respect des contraintes fonctionnelles, techniques et réglementaires :
1) Construire avec les différentes parties prenantes le protocole d'évaluation
2) Exécuter le protocole d'évaluation

Boîte à outils

- Protocole d'évaluation/cadre de test
- Métriques métiers et Data Science
- Outils de benchmarking
- Outils de détection de biais
- Outil(s) d'IHM, de contrôle humain

3. Sélection du modèle

- **Construction d'un protocole de sélection de modèle** avec les différentes parties-prenantes et déploiement

Boîte à outils

- Métriques métiers et Data Science
- Outils d'explicabilité et quantification d'incertitude

Notre *check-list* pour vous aider à opérationnaliser le RIA

- ❑ Mise à jour des **Fiches sur les jeux de données (d'entraînement, validation, test) utilisés, présentant le processus de prétraitement (art. 11, annexe IV, §2)**
- ❑ Mise à jour de la **Documentation technique du modèle**
- ❑ **Stratégie de gestion des logs**
- ❑ **Processus en place pour le déploiement du contrôle humain**
- ❑ Mise à jour de la **Notice d'utilisation pour les déployeurs**

❑ **Intégration Documentation technique**
1) Protocole d'évaluation : ensemble des expérimentations à conduire pour atteindre les exigences attendues et respecter les contraintes (précise l'interaction et intervention humaine)
2) Résultats du protocole d'évaluation : tableau de suivi des métriques et des biais par expérimentation

❑ **Intégration Documentation technique**
Procédures de validation et d'essai utilisées, y compris les informations sur les données (Annexe 4 2.g) **– documenter le choix du modèle sur la fiche projet**

IHM : Interface Homme-Machine

HUB FRANCE .IA

RIA – Opérationnalisation

MODÉLISATION – FOCUS *GPAI*

1. Construction du modèle

Obligations incombant aux fournisseurs de modèles d'IA à usage général (Art. 53)*

- Établir et tenir à jour la documentation technique du modèle.
- Élaborer, tenir à jour et mettre à disposition la documentation permettant de bien comprendre les capacités et les limites du modèle *GPAI*.
- Assurer le respect des lois européennes sur les droits d'auteur.
- Fournir le résumé détaillé de la donnée d'entraînement du modèle *GPAI*.

Les obligations énoncées ne s'appliquent pas aux modèles d'IA qui sont publiés en licence libre et ouverte sauf s'ils présentent un risque systémique (Art. 53.2)

*Potentiellement étendues aux entreprises qui *in fine-tune* un modèle *GPAI*, exclusivement sur les parties modifiées/ nouvellement introduites (Cons. 109)

Boîte à outils

- Standard de construction du modèle
- Template de documentation du modèle
- Modèle de résumé des données d'entrainement du modèle *GPAI* (fourni par le Bureau de l'IA)
- Template de la déclaration de respect des lois européennes sur les droits d'auteur.

2. Évaluation du modèle

- **Classifier** des systèmes présentant **un risque systémique** (Art. 51), informer la Commission et/ou présenter les éléments pour demander une exemption (si applicable – Art. 52).
- Obligations complémentaires : évaluation du modèle et piste d'audit des tests.

Boîte à outils

- **NA**

3. Sélection du modèle

- **Optionnel :** v. le code de conduite interne si défini et applicable.

Boîte à outils

- **NA**

Notre *check-list* pour vous aider à opérationnaliser le RIA

- ❑ **Documentation technique du modèle GPAI,** y compris la description des limites et des faiblesses
- ❑ **Description des données** utilisées pour entrainer le *GPAI*.
- ❑ **Déclaration** de respect des lois européennes sur les droits d'auteur.
- ❑ **Notification à la Commission européenne** (modèle *GPAI* à risque systémique)
- ❑ Définition d'un **mandataire** établi dans l'UE (si applicable)

- ❑ NA

- ❑ NA

HUB FRANCE IA

RIA – Définitions clés

Documentation technique du SIA

Définition

Conformément à l'article 11 et à l'annexe IV du RIA, les fournisseurs des SIA à **haut risque** doivent établir une **documentation technique avant la mise sur le marché ou la mise en service** du système. Le déployeur doit, quant à lui, vérifier que le fournisseur a bien mis en place la documentation technique. Cette documentation doit être tenue à jour de manière continue. Les exigences relatives aux informations minimales à inclure dans le document figurent à l'annexe IV. Toutefois, si nécessaire, ces exigences peuvent être modifiées par des actes délégués de la Commission européenne (art. 97) en fonction des évolutions technologiques.

1. Description générale du SIA :

- ❑ **destination et informations d'identification :** comprend l'objectif visé, le nom du fournisseur, la version du système et son lien avec les versions précédentes ;
- ❑ **compatibilité :** explication de la manière dont le système interagit avec d'autres matériels ou logiciels, y compris d'autres SIA ;
- ❑ **formats disponibles :** description des différentes formes sous lesquels le système est proposé, comme les logiciels téléchargeables ou les API.

2. Aspects techniques et développement :

- ❑ **processus de développement :** méthodes utilisées, incluant l'intégration de systèmes préexistants/pré-entraînés ou d'outils tiers ;
- ❑ **conception et logique :** spécifications des algorithmes, objectifs d'optimisation et choix techniques effectués pour respecter les exigences réglementaires ;
- ❑ **architecture :** organisation des composants logiciels et ressources informatiques utilisées pour l'entraînement et la validation ;
- ❑ **stress-test et cyber :** liste des techniques visant à assurer la robustesse, la résilience et la cybersécurité des systèmes (art. 15 – voir focus).

Focus article 15 – Exactitude, robustesse et cybersécurité

Cet article exige que les SIA à haut risque soient déployés avec des niveaux d'exactitude, de robustesse et de cybersécurité appropriés et alignés sur leurs risques. Voici une liste des principaux éléments requis par cet article :

- élaborer un système, résilient face aux erreurs, aux défaillances ou aux incohérences, visant à atteindre un niveau approprié de précision, de robustesse et de cybersécurité, en s'appuyant sur des critères de référence et des méthodes de mesure appropriés ;
- Pour les systèmes qui continuent à apprendre tout au long de leur cycle de vie, accorder une attention particulière à la dégradation de la performance et l'apparition potentielle des biais ;
- assurer que le système soit résistant aux tentatives de modification de son utilisation, de ses résultats ou de ses performances par des tiers non autorisés et malveillants qui tentent d'exploiter les faiblesses du système ;
- documenter les mesures visant à remédier aux vulnérabilités propres à l'IA qui comprennent, le cas échéant, des mesures de prévention, de détection, de réponse, de résolution et de contrôle de l'empoisonnement des données et des modèles, des attaques adverses et de l'évasion de modèle.

Ces informations doivent figurer dans la documentation technique. Néanmoins, le niveau de détail de ces éléments n'a pas été spécifié, laissant la porte ouverte à l'interprétation dans l'attente d'éventuelles clarifications fournies par les normes harmonisées (à date prévue pour S2 2026)

HUB FRANCE IA

RIA – Définitions clés

Documentation technique du SIA

Définition

3. Données et gestion (art. 10) :

- ❑ **bases de données** : informations et exigences relatives aux données d'entraînement, validation et d'essai, avec description de leur provenance, caractéristiques principales et méthode de sélection;
- ❑ **collecte/traitement des données** : fiches techniques détaillant les méthodes utilisées pour collecter et traiter les données.

4. Compatibilité et interface utilisateur (production) :

- ❑ **matériel supporté :** description des équipements sur lesquels le SIA peut fonctionner ;
- ❑ **interface utilisateur :** présentation des fonctionnalités mises à disposition des utilisateurs finaux, avec des guides d'utilisation pour les déployeurs ;
- ❑ **contrôle humain :** évaluation des mesures de contrôle humain nécessaires (art. 14).

5. Conformité et mise à jour :

- ❑ **déclaration de conformité :** copie de la déclaration UE de conformité (art. 47) ;
- ❑ **gestion des risques** : description détaillée du système de gestion des risques (art. 9) ;
- ❑ **mises à jour :** exigences relatives aux versions logicielles et aux micrologiciels, y compris les besoins en mises à jour ;
- ❑ **références :** liste des normes harmonisées appliquées, en cas d'absence description détaillée des solutions adoptées pour satisfaire aux exigences relatives aux SIA à haut risque, avec des références à d'autres normes ou références techniques utilisées.
- ❑ **photographies et illustrations :** documentation visuelle pour identifier les caractéristiques externes et internes des produits intégrant le SIA (si applicable).

6. Monitoring et suivi du système :

- ❑ **modifications et incidents :** enregistrement des modifications apportées au SIA au long de son cycle de vie, incidents observés et test effectués ;
- ❑ **surveillance après commercialisation :** description de la solution de contrôle des performances après commercialisation et son plan de surveillance.

Cas particuliers :

- Pour les PME et les jeunes entreprises, il est possible d'établir une **version simplifiée** de la documentation, en suivant un modèle qui sera établi par la Commission ;
- Pour les systèmes déjà couverts par une législation d'harmonisation de l'UE (section A, annexe I), il convient de noter que la documentation à produire doit contenir les informations requises par le RIA (annexe IV) ainsi que les informations requises en vertu de ces réglementations sectorielles.

HUB FRANCE IA

RIA – Définitions clés

Notice d'utilisation

Définition

L'article 13 du RIA impose aux fournisseurs des SIA à **haut risque** de fournir un guide détaillé pour l'utilisateur final : la « notice d'utilisation » (art. 3 pt. 15), incluant les éléments suivants :

1. Description générale :

- ❑ **finalités :** description claire des tâches que le SIA est conçu pour accomplir ;
- ❑ **informations de contact :** l'identité et les coordonnées du fournisseur (ou mandataire) ;
- ❑ **Performance attendue :** documentation du niveau d'exactitude, de robustesse et de cybersécurité (visé à l'art. 15), référence pour les tests et la validation du SIA, incluant les circonstances pouvant influencer ces niveaux ;
- ❑ **data :** spécifications concernant les données d'entrée, ainsi que toute autre information pertinente sur les jeux de données d'entraînement, de validation et de test utilisés.

2. Instructions pour une utilisation correcte :

- ❑ **conditions d'utilisation et limitations :** indication des cas d'utilisation prévus et des contextes dans lesquels le système peut être utilisé et liste des scénarios connus d'utilisation inappropriée potentiellement risquée pour l'utilisateur ;
- ❑ **évolutions :** liste des modifications du SIA et de sa performance qui ont été prédéterminées par le fournisseur au moment de l'évaluation initiale de la conformité afin de qualifier une potentielle modification substantielle.

3. ressources et maintenance :

- ❑ **ressources et durée de vie :** les ressources informatiques et matérielles nécessaires pour le bon fonctionnement du système et sa durée de vie attendue ;
- ❑ **entretien :** instructions pour assurer le bon fonctionnement du système sur le long terme, y compris les mises à jour logicielles.

4. Transparence et traçabilité :

- ❑ **explicabilité :** capacités techniques du SIA de produire des informations pertinentes pour expliquer ses sorties, ainsi que des éléments permettant aux déployeurs d'interpréter et d'utiliser ces sorties de manière appropriée ;
- ❑ **contrôle humain (art. 14) :** mesures techniques mises en place pour permettre la supervision des sorties des SIA ;
- ❑ **process de journalisation :** collecte, stockage et interprétation des logs générés pour assurer la traçabilité des décision prises par le SIA.

HUB FRANCE IA

VIII. Production

VIII. PRODUCTION

VIII.1 Introduction

L'objectif de cette phase est de déployer le SIA dans un environnement réel afin qu'il puisse traiter des données en conditions opérationnelles et fournir des résultats exploitables. La phase de production doit comprendre également la surveillance et la maintenance continues du système.

Cette étape doit s'appuyer sur un préalable nécessaire : la description de l'infrastructure de production ainsi que des modalités prévues pour le déploiement et l'exploitation du système.

VIII.2 Deploiement du systeme

Après avoir développé et évalué le SIA, celui-ci doit être déployé dans son environnement de production. Des mesures correctives peuvent être nécessaires afin de garantir la performance et la robustesse du modèle et de maintenir l'alignement de la pertinence du système aux besoins métier.

Tout d'abord, il est nécessaire de **définir et dimensionner l'infrastructure de production** du SIA et d'effectuer une analyse des **risques de cybersécurité** susceptibles d'être engendrés ou amplifiés par son déploiement.

Ensuite, il convient notamment de mettre en place l'**infrastructure *CI/CD***[16], de déployer l'infrastructure nécessaire, d'effectuer les tests prévus et, enfin de déployer le modèle en production.

Une mise à jour du *versioning* sera également nécessaire, ainsi que la mise à jour de la documentation du système.

[16] *CI/CD (Continuous Integration/Continuous Delivery)* est la combinaison des pratiques d'intégration continue et de livraison continue ou de déploiement continu.

Pour ce faire il est impératif de s'appuyer sur la stratégie de déploiement d'un SIA (standard), sur les outils de gestion et de déploiement des modèles (*MLflow*[17]*, Kubeflow*[18]*, Comet*[19]*, Bento ML*[20] *etc.*) ainsi que sur les outils de versionnage.

Du point de vue de la documentation de conformité, une mise à jour de la documentation technique du système est nécessaire à chaque étape du processus de déploiement.

VIII.3 SURVEILLANCE DU SYSTEME

C'est lors de cette phase qu'il est nécessaire de mettre en place une surveillance du système par la supervision en continu, ce qui permet de garantir, dans la durée, la qualité des données, la performance du modèle et l'intégrité du système.

A cette étape, il faut tout d'abord définir la stratégie de supervision du SIA et de maintien de son intégrité en matière de cybersécurité. Pour cela, il convient notamment de définir les indicateurs de performance du modèle et les seuils d'action, c'est-à-dire les niveaux de dégradation à partir desquels une action corrective doit être engagée, d'établir le plan de mise à jour et de maintenance du modèle et de définir les métriques d'utilisation.

Cette surveillance doit permettre de détecter au plus tôt les éventuelles dégradations des données, des performances ou de l'intégrité du système et de déclencher les actions correctives nécessaires.

Pour les SIA à haut risque, des exigences spécifiques du RIA doivent notamment être prises en compte :

- **vérifier** tout au long de l'exploitation du système, les entrées et les sorties afin de détecter au plus tôt les anomalies ou incidents, notamment lorsque les données d'entrée ou les résultats produits apparaissent aberrants ;

[17] MLflow Project, a Series of LF Projects, LLC. MLflow - Open Source AI Platform for Agents, LLMs & Models. *MLflow AI Platf*. 2025. https://mlflow.org
[18] The Kubeflow Authors. Kubeflow. *Kubeflow*. 2026. https://www.kubeflow.org/
[19] Comet ML, Inc. Docs Home - Comet Docs. 2026. https://www.comet.com/docs/v2/
[20] Atalaya Inc. Bento: Run Inference at Scale. 2026. https://www.bentoml.com/

- effectuer des contrôles réguliers (**audits**) et documenter leurs résultats, notamment au moyen de rapports d'audit lorsque cela est prévu par les procédures applicables ;
- définir et mettre en place un **dispositif de supervision humaine** permettant de surveiller le fonctionnement du SIA, notamment au regard de ses résultats, des données utilisées et des éventuels biais. Cette exigence est notamment prévue à l'article 14.4 a du RIA pour les SIA à haut risque[21] ;
- garantir que le système permet, d'un point de vue technique, l'**enregistrement automatique des événements (*logs*)**, comme prévu par l'article 12 b du RIA. Ceci favorise la traçabilité et permet notamment de faciliter la **surveillance après commercialisation,** et d'évaluer d'autres risques susceptibles d'apparaître tout le long du cycle de vie (Art. 72.1 & 9.2 c).

Les exigences techniques applicables à ces différents dispositifs pourront être précisées par les normes harmonisées pertinentes.

La mise en place d'une surveillance du système permet également d'effectuer les signalements aux autorités de surveillance compétentes en cas d'incident ou de risque d'incident repéré (art. 20).

Pour cette étape de surveillance du système, il est possible de s'appuyer sur des outils spécifiques mis en place pour favoriser la surveillance du système, tels que :

- **le protocole de surveillance continue** : définition des processus de surveillance, des responsabilités, des modalités de remontée des incidents et des actions de reprise prévues ;
- **les outils de gestion des alertes** (boîtes mail, *ticketing*, alertes, notifications) : il faut indiquer quand les alertes sont remontées (la gestion des seuils de déclenchement doit éviter l'effet « arbre de Noël » où trop d'alertes sont remontées) et qui doit prendre la responsabilité des mesures de remédiation ;
- **les outils de quantification d'incertitudes** : les SIA sont probabilistes et donc les sorties portent toujours un certain degré d'incertitude. Il faut préciser les barres d'erreur acceptables ;

[21] Le contrôle humain est également considéré comme un principe de l'IA de confiance, associé à une démarche éthique propre à chaque organisation.

- **les outils de monitoring de *biais*** : les biais doivent être mesurés et les dégradations remontées si elles dépassent les seuils (« incident ») ;
- **le système de gestion des *logs*** : on doit définir précisément les événements qui seront logués, la fréquence d'enregistrement, la durée de rétention des logs enregistrés ;
- **le protocole de signalement des incidents** doit préciser la fréquence de signalement des incidents identifiés et la/les personnes qui doivent être notifiées (ceci dépendra des normes sectorielles).

En ce qui concerne la check-list documentaire à remplir à cette étape pour être conforme à la réglementation, elle se compose des éléments suivants :

- le registre des *logs* automatiques du système ;
- le protocole de surveillance continue (art. 72) ;
- les rapports sur les résultats des contrôles réguliers (audits) ;
- lorsque l'organisation intervient en qualité de **fournisseur**, la mise à jour de la notice d'utilisation destinée aux **déployeurs**, notamment en ce qui concerne les mesures de suivi et de surveillance à respecter ;
- la mise à jour de la documentation technique (annexe IV, .3).

VIII.4 Maintenance du systeme

A cette étape il est nécessaire de prévoir la maintenance du système sur la base des résultats de la surveillance, des incidents identifiés et des contrôles réalisés.

En fonction des incidents remontés et des contrôles, on devra décider, ou pas, de relancer l'entraînement du modèle, voire d'adapter le système. Si nécessaire, on prendra des mesures correctives afin d'assurer la performance et la robustesse du modèle et maintenir l'alignement de la pertinence du système aux besoins métier. En cas d'incident, il peut être nécessaire de mettre en place des mesures correctives pour garantir la conformité du système (art. 73).

Pour ce faire, il est nécessaire de s'appuyer sur le **process interne de gestion et maintenance des SIA**.

Afin d'être conforme à la réglementation, si on a un rôle de fournisseur du système, il est également nécessaire de mettre à jour la **notice d'utilisation à l'attention des**

déployeurs, avec les mesures de maintenance nécessaires pour assurer le bon fonctionnement du système.

RIA – Opérationnalisation

PRODUCTION (1)

Déployer le système dans un environnement réel afin qu'il puisse traiter des données en direct et fournir des résultats exploitables. La phase de production doit inclure la surveillance et la maintenance continue.

Déploiement du système

Prendre des mesures correctives afin d'assurer la performance et la robustesse du modèle et maintenir l'alignement de la pertinence du système aux besoins métier.

Surveillance du système

Supervision en continu de la qualité des données, la performance du modèle et l'intégrité du système.

Maintenance du système

Prendre des mesures correctives afin d'assurer la performance et la robustesse du modèle et maintenir l'alignement de la pertinence du système aux besoins métier.

(1) La phase et les étapes font référence au livrable « Opérationnaliser la gestion des risques » du *GT Banque* du Hub France IA.

HUB FRANCE .IA

RIA – Opérationnalisation

PRODUCTION

Préalables nécessaires

- **Description de l'infrastructure de production et des modalités de déploiement**

Notre *check-list* pour vous aider à opérationnaliser le RIA

1. Déploiement

- Définir et dimensionner **l'infrastructure de production** du SIA
- Effectuer une analyse des potentiels risques cyber
- Déployer une infrastructure **CI/CD**
- Déployer l'infrastructure, effectuer les tests unitaires, déployer le modèle en production
- **Mettre à jour le versioning**
- **Compléter la documentation**

Boîte à outils

- Stratégie de déploiement d'un SIA (Standard)
- Outils de gestion et de déploiement des modèles (MLflow, Kubeflow, Comet, Bento ML etc.)
- Outils de versioning

→

- *Mise à jour de la* **Documentation technique du système**

2. Surveillance du système

- Définir une stratégie de supervision du SIA et de son intégrité cyber.
- Vérifier les entrées et les sorties du modèle (monitoring)
- Décrire les indicateurs de performance et des seuils d'action, établir le plan de mise à jour et de maintenance du modèle, définir les métriques d'utilisation
- **Définir et mettre en place un contrôle humain**, afin de surveiller le fonctionnement du SIA (données, biais, etc.) (Art. 14.4 a)
- Assurer la tenue des logs automatiques du système (Art. 12 b)
- Évaluer d'autres risques susceptibles d'apparaître (système de surveillance post-commercialisation) (Art. 72.1 & 9.2 c)
- Si incident, ou risque d'incident, signalement aux autorités de surveillance (Art. 20)

- Protocole de surveillance continue
- Outils de gestion des alertes (boîtes mail, ticketing, alertes, notifications)
- Outils de quantification d'incertitudes
- Outils de monitoring de biais
- Système de gestion des logs
- Protocole de signalement des incidents, (v. normes sectorielles)

→

- Registre des Logs automatiques du système
- **Protocole de surveillance continue** (Art. 72)
- Rapport sur les résultats des contrôles réguliers (audits)
- **Notice d'utilisation** à l'attention des déployeurs : mesures de suivi/surveillance
- Documentation technique (Annexe IV, .3)

3. Maintenance du système

- Go/No Go re-entraînement du modèle ou adaptation du système
- Si nécessaire, mesures correctives (Art. 73)

- Process interne de gestion et maintenance des SIA

→

- *Mise à jour de la* **Notice d'utilisation** à l'attention des déployeurs, avec les mesures de maintenance nécessaires pour assurer le bon fonctionnement du système

HUB FRANCE IA

IX. Transfert au métier

IX. TRANSFERT AU METIER

IX.1 Introduction

L'objectif de cette phase est d'intégrer le SIA dans le processus métier au sein de l'organisation et d'accompagner la transformation liée aux nouveaux usages auxquels ce système répond, afin d'assurer une transition fluide vers l'exploitation réelle et une utilisation concrète, et garantir que l'innovation technique soit alignée avec les exigences métier.

IX.2 Identifier les roles

Le transfert au métier comporte tout d'abord la nécessité identifier les utilisateurs du système et en définir les responsabilités. Cette première étape est cruciale pour définir la gouvernance humaine autour du SIA et évaluer les risques liés à l'usage du système de la part des différentes populations concernées.

Cette étape commence par une distinction précise entre les différents types d'acteurs : d'une part, les **utilisateurs du SIA**, qui sont les clients internes manipulant l'outil au quotidien, et d'autre part, le cas échéant, les **bénéficiaires** ou **utilisateurs finaux** (clients externes) qui peuvent être impactés par les décisions de l'IA sans pour autant l'utiliser directement[22].

Pour formaliser cette identification, l'entreprise peut s'appuyer sur un **annuaire des rôles et responsabilités,** tout en veillant à ce que la « **Fiche projet** » soit mise à jour pour refléter cette organisation humaine.

IX.3 Accompagner la transformation

Dans un deuxième temps, le transfert au métier doit être accompagné et ne peut réussir sans un effort important de formation et de communication, visant à ga-

[22] Souvent, les utilisateurs du système peuvent coïncider avec les bénéficiaires lorsque le système n'est utilisé que pour des besoins internes et n'est pas accessible aux clients.

rantir la maîtrise technique du système et un climat de confiance vis à vis des nouveaux process et des résultats. Pour ce faire, des actions de formation/acculturation spécifiques à l'usage visé doivent être définies et appliquées.

Le processus métier lui-même doit subir une **validation et un réglage final** pour s'assurer que l'IA s'y imbrique parfaitement, **tout en veillant à « embarquer »** psychologiquement et stratégiquement les collaborateurs dans ce nouveau dispositif. Un volet essentiel concerne la **formation aux usages** : il ne suffit pas de montrer comment le système fonctionne, il faut aussi être d'une transparence totale sur ses **capacités et surtout ses limites**, ainsi que sur les **exigences réglementaires et éthiques** qui l'accompagnent, afin d'éviter toute utilisation non conforme et contraire aux valeurs de l'organisation. Sur le plan documentaire et réglementaire, cela se traduit par :

- la distribution d'un **guide utilisateurs** et la mise en œuvre des obligations du RIA, notamment l'**article 50** sur l'information des utilisateurs (si applicable) ;
- la **Notice d'utilisation** demandée par l'**article 13** concernant les SIA à haut risque.

Tous ces éléments doivent s'articuler avec les dispositions de l'organisation visant à répondre à l'Article 4 concernant la maîtrise de l'IA. Les **politiques internes relatives à la donnée, l'IA, l'éthique/droits fondamentaux**, à la fois généralistes et spécifiques à la filière métier sont indispensable pour l'accompagnement de ces nouveaux usages.

Si le dispositif touche des clients externes, il sera nécessaire de communiquer auprès d'eux que autour du **dispositif et les garanties de fiabilité et confiance**.

Pour finaliser l'étape d'accompagnement de la transformation, il est indispensable de consolider plusieurs documents de référence garantissant la maîtrise du système. Cette phase comporte la mise à jour de la **Notice d'utilisation**, conformément aux exigences de l'**article 13** du RIA (si applicable). Parallèlement, la mise en place d'un **guide utilisateurs** constitue une bonne pratique essentielle pour orienter quotidiennement les équipes dans leurs nouvelles méthodes de travail. Enfin, l'entreprise doit être en mesure de fournir des preuves concrètes, tant pour attester de la **formation effective des parties prenantes** au nouveau processus métier que pour démontrer l'information des utilisateurs et des bénéficiaires (si applicable) via les mentions d'information.

IX.4 Évaluer les usages

Une fois le système en place, la phase de « transfert métier » prévoit un mécanisme de surveillance pour évaluer l'adéquation des nouveaux usages, par rapport aux besoins métiers et aux métriques associées qui ont été préalablement définis et documentés au sein de la « **fiche projet** ».

Il est nécessaire de procéder à une **évaluation périodique** pour vérifier si le SIA est toujours en adéquation avec les exigences du projet, en se basant sur des **métriques métier**. Ce pilotage est supporté par l'utilisation d'une **liste de métriques métier** (par exemple, gains de productivité, satisfaction client) et d'une **liste de métriques techniques** (par exemple, précision, *recall, F1-Score* – cf. Fiche projet). Un point de vigilance majeur est souligné : si l'on constate un décalage entre les attentes métier (métriques métier) et les performances du système (métriques techniques de data science), il ne faut pas hésiter soit à **remettre en cause la pertinence des indicateurs, métiers ou techniques,** ou à **retourner à l'étape de modélisation**. Ce processus s'appuie sur un **outil de suivi des indicateurs et des métriques** et aboutit à la mise à jour de la **fiche projet.**

RIA – Opérationnalisation

Transfert au métier[1]

Intégrer le système d'IA dans le processus métier au sein de l'entreprise et accompagner la transformation liée aux nouveaux usages.

Identifier les rôles	**Identifier les utilisateurs du système et en définir les responsabilités**
Accompagner la transformation	**Mettre en place des actions de formation/acculturation spécifiques à l'usage**
Evaluer les usages	**Evaluer l'adéquation des usages par rapport aux besoins métiers et aux métriques associées**

(1) La phase et les étapes font référence au livrable « Opérationnaliser la gestion des risques » du GT Banque du Hub France IA Hub-France-IA-Operationnaliser-la-gestion-des-risques.pdf

HUB FRANCE .IA

RIA – Opérationnalisation

Transfert au métier

	Boîte à outils	Notre *check-list* pour vous aider à opérationnaliser le RIA
1. Identifier les rôles • Identifier les **utilisateurs** du SIA (clients internes) • Identifier les **bénéficiaires/utilisateurs finaux** (clients externes) du SIA, si différents des utilisateurs	• **Annuaire** des rôles et responsabilités	• Mettre à jour la **Fiche projet** (2)
2. Accompagner la transformation • **Validation et réglage** final du nouveau process • **Embarquer les utilisateurs** dans la stratégie de mise en place du nouveau process ou dispositif • **Formation** des utilisateurs aux **usages, limites et capacités du SIA** • **Distribution d'un guide utilisateurs aux parties prenantes** • Mettre en place un **dispositif d'information** des utilisateurs et des bénéficiaires, si applicable (Art. 50) • **Communication** auprès des bénéficiaires éventuels concernant le dispositif et les garanties de fiabilité et confiance	• **Politiques internes** de la filière métier relatives à la Data, l'IA et l'éthique/droits fondamentaux • **Template des mentions d'information** • **Kit de communication**	• Mise à jour de la **Notice d'utilisation** (Art. 13) • Mise en place d'un **guide utilisateurs** (bonne pratique) • **Preuve de formation** des parties prenantes sur le nouveau process • Preuve d'implémentation des **mentions d'information**
3. Evaluer les usages • **Evaluer périodiquement la pertinence métier du SIA** par rapport aux métriques métier (adéquation avec les besoins métier) • Si non adéquation des métriques métiers et des métriques techniques, **remettre en cause les métriques techniques** et revenir à la phase de modélisation	• Liste des **métriques métier** (v. étape objectifs métier) • Liste des **métriques techniques** (data science) • **Outils de suivi** des indicateurs et des métriques	• Mise à jour de la **Fiche projet** (2) **(métriques métier et data science)**

(2) L'explication détaillée de la Fiche Projet est disponible dans le feuillet « définition d'un projet »

HUB FRANCE IA

X. Certification

X. CERTIFICATION

X.1 INTRODUCTION

L'évaluation de conformité permet de **garantir** que les SIA à haut risque respectent les exigences essentielles de sécurité, de robustesse technique et de protection des droits fondamentaux avant leur mise sur le marché ou leur mise en service (considérant 123).

Ce processus, défini à l'article 43, permet au fournisseur de vérifier la conformité de son système aux obligations de la section 2. À l'issue de cette évaluation, il peut **établir une déclaration UE de conformité** (article 47), l'apposer sur le système sous forme de **marquage CE** (article 48) et en **assumer la responsabilité juridique**. La déclaration doit être tenue à disposition des autorités compétentes pendant dix ans.

L'évaluation de conformité s'impose principalement aux fournisseurs (article 16), mais également aux importateurs, distributeurs ou déployeurs qui modifient substantiellement un système existant (article 25).

Cette évaluation peut résulter de **différentes procédures prévues à l'article 43** en fonction des SIA visés soit à l'annexe I soit à l'annexe III et selon si le fournisseur a appliqué les normes harmonisées visées à l'article 40 ou les spécifications communes visées à l'article 41. Il en existe deux : un contrôle interne prévu à l'annexe VI et un contrôle par un organisme notifié (annexe VII).

L'article 42 introduit une **présomption de conformité** à certaines exigences. La première étant l'obligation de l'article 10 lorsque le SIA à haut risque a été formé et testé sur des données reflétant le cadre géographique, comportemental, contextuel ou fonctionnel spécifique dans lequel il est destiné à être utilisé. La seconde est une présomption de conformité à l'article 15 lorsque le SIA à haut risque a été certifié dans le cadre d'un dispositif de cybersécurité conformément au règlement (UE) 2019/881 et dont les références ont été publiées au Journal officiel de l'Union européenne.

Des **dérogations temporaires** sont prévues à l'article 46 pour des motifs d'urgence ou de sécurité publique, sous conditions strictes.

Enfin, la mise en œuvre des normes harmonisées par le CEN-CENELEC, attendue pour fin 2025, constitue un défi central en termes de planning (les normes sont issues d'un process long qui garantit le consensus et fin 2025 le constat est un retard non maîtrisé), en termes de qualité (par la représentativité et l'expertise des acteurs qui y participent) et finalement en termes de légitimé au niveau international. Elles doivent être validées par la Commission européenne et publié aux JO pour commencer à être utilisable par les acteurs pour leur conformité.

Leur adoption facilitera la conformité pour les organisations en Europe mais n'enlèvera pas le besoin de suivi des cadres internationaux (par exemple le standard ISO42001 combiné au cadre de gestion des risques du NIST sont reconnus par les acteurs internationaux).

HUB FRANCE IA

L'ÉVALUATION DE CONFORMITÉ SELON LE RIA

Évaluation de conformité

Vise à garantir que les systèmes sont sûrs, robustes et respectent les droits fondamentaux

- Systematic procedure verifying if an AI system complies with the requirements of the **AI Act**
- If the evaluation is suc**cessful, the provider must issue a declaration of conformity**, or **if applicable, an accreditation certificate is provided by the notified body**.
- These documents confirm that the product meets all applicable standards and allows the **CE marking** to be applied.
- The provider must then **register the** system in the EU database.

Traçabilité de la conformité :
Cette procédure permet aux autorités de surveillance de **tracer le produit** et d'en vérifier la **conformité tout au long de sa durée de vie** sur le marché. Tout incident ou modification majeure devra être signalé.

Applicabilité de l'évaluation de conformité

Applicable principalement aux fournisseurs de système d'IA

Applicable aux **SIA à haut risque** (Ann. III du RIA).

Exemples :

- l'emploi et la gestion des ressources humaines (y compris formation) ;
- les services publics essentiels ;
- les infrastructures critiques et les systèmes de sécurité ;
- les systèmes utilisés dans le cadre de missions de sécurité intérieure ;
- les systèmes biométriques.

Modification substantielle :
Les distributeurs, importateurs et déployeurs sont considérés comme des fournisseurs lorsqu'ils apportent une **modification substantielle** d'un SIA déjà mis sur le marché (Art. 25 RIA).

Les 2 types d'évaluation de conformité

Auto- évaluation (contrôle interne)

Pour certains **SIA à haut risque** répertoriés dans l'**Annexe III**, l'entreprise procède à sa propre évaluation interne du SIA. Une fois cette évaluation effectuée, le fournisseur émet une **Déclaration de Conformité**.

Évaluation par un tiers (organisme notifié)

Pour les SIA répertoriés dans l'**Annexe I**, une **évaluation de la conformité par un organisme notifié (tiers indépendant)** est obligatoire. A l'issue de cette évaluation, l'organisme notifié émet un certificat de conformité.

Présomption de conformité :
Les SIA utilisés dans des secteurs qui sont déjà soumis à une **réglementation sectorielle stricte** bénéficient d'une **présomption de conformité** si ces cadres législatifs intègrent des **normes équivalentes aux exigences du RIA.**

HUB FRANCE .IA

L'ÉVALUATION DE CONFORMITÉ SELON LE RIA

LISTE NON-EXHAUSTIVE

Type de système d'IA	Évaluation de conformité applicable	Référence textuelle
SIA à haut risque	Évaluation par un organisme notifié pour les systèmes relatifs à la biométrie, à défaut de normes harmonisées ou spécifications communes	*Article 43; Annexe III, point 1*
	Auto-évaluation possible pour les systèmes relatifs à la biométrie si application des normes harmonisées ou spécifications communes	
	Auto-évaluation possible pour certains systèmes à haut risque relevant des points 2 à 8 de l'Annexe III	*Article 43; Annexe III, point 2 à 8*
SIA à haut risque couverts par Législation d'Harmonisation de l'UE	Conformité selon la procédure prévue par la législation d'harmonisation de l'UE applicable	*Article 43; Annex I*
	Auto-évaluation possible si les normes harmonisées sont appliquées	*Article 43; Annex I*
SIA utilisés par les autorités publiques	Pour les autorités répressives, les services de l'immigration / d'asile ou par les institutions de l'UE, **l'autorité de surveillance du marché agit en tant qu'organisme notifié**. C'est une exception au principe général que le fournisseur peut choisir n'importe lequel des organismes notifiés	*Article 43; Annex III*

HUB FRANCE IA

Bibliographie

X.3 Bibliographie

Atalaya Inc. Bento: Run Inference at Scale. 2026. https://www.bentoml.com/

Comet ML, Inc. Docs Home - Comet Docs. 2026. https://www.comet.com/docs/v2/

Commission Européenne. La Commission publie des lignes directrices sur la définition des systèmes d'IA afin de faciliter l'application des règles de la première législation sur l'IA | Bâtir l'avenir numérique de l'Europe. 6 février 2025. https://digital-strategy.ec.europa.eu/fr/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application

Commission européenne. La Commission publie les lignes directrices sur les pratiques interdites en matière d'intelligence artificielle (IA), telles que définies par la législation sur l'IA. | Bâtir l'avenir numérique de l'Europe. 4 février 2025. https://digital-strategy.ec.europa.eu/fr/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act

Commission européenne. Le code de bonnes pratiques de l'IA à usage général | Bâtir l'avenir numérique de l'Europe. 31 juillet 2026. https://digital-strategy.ec.europa.eu/fr/policies/contents-code-gpai

Commission européenne. Lignes directrices à l'intention des fournisseurs de modèles d'IA à usage général | Bâtir l'avenir numérique de l'Europe. 28 avril 2026. https://digital-strategy.ec.europa.eu/fr/policies/guidelines-gpai-providers

European Union Agency for Fundamental Rights. Charte des droits fondamentaux de l'Union européenne | Article 21 - Non-discrimination |. Journal officiel de l'Union européenne C 303/17. 14 décembre 2007. https://fra.europa.eu/fr/eu-charter/charter/article/21-non-discrimination

Hub France IA. Livre blanc : Contrôle des risques des systèmes d'Intelligence Artificielle. Octobre 2022. https://www.hub-franceia.fr/wp-content/uploads/2022/10/22_10_19_Controle-des-risques-des-systemes-IA_PDF.pdf

Hub France IA. Livre blanc : Opérationnaliser la gestion des risques des systèmes d'intelligence artificielle. Juillet 2024. https://www.hub-franceia.fr/wp-content/uploads/2024/07/Hub-France-IA-Operationnaliser-la-gestion-des-risques.pdf

MLflow Project, a Series of LF Projects, LLC. MLflow - Open Source AI Platform for Agents, LLMs & Models. *MLflow AI Platf.*. 2025. https://mlflow.org

Parlement Européen, Conseil de l'Union européenne. Règlement (UE) 2024/1689 du Parlement Européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) no 300/2008, (UE) no 167/2013, (UE) no 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle), *2024/1689*. 12 juillet 2024. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L_202401689

The Kubeflow Authors. Kubeflow. *Kubeflow.* 2026. https://www.kubeflow.org/

HUB FRANCE IA

Annexe : Checklist pour vous aider à opérationnaliser le RIA

OPERATIONNALISATION DU RIA
Septembre 2026

X.4 ANNEXE : *CHECKLIST* POUR VOUS AIDER À OPÉRATIONNALISER LE RIA

Vous trouverez ci-dessous une liste de contrôle reprenant les principaux éléments à produire tout au long du projet. Pour la liste complète et détaillée, veuillez-vous reporter aux feuillets, aux fiches de définition et aux sections du livret blanc. Nous vous rappelons également que tous les livrables présentés ici ne sont pas nécessaires pour chaque SIA, mais dépendent des axes de risque associés (haut risque, exigence de transparence (art. 50), intégration d'un modèle *GPAI*) :

- fiche projet (cf. fiche dédié) ;
- documentation technique (cf. fiche dédié) ;
- notice d'utilisation (cf. fiche dédié) ;
- preuves de formation d'acculturation IA des salariés ;
- politique de gestion des risques ;
- politique, procédures et instructions concernant la gestion des données ;
- fiche sur les jeux de données ;
- stratégie de gestion des logs et registre associé ;
- protocole de surveillance continue et rapport des contrôles effectués.

Spécifiquement pour les fournisseurs (ou modificateurs) de modèles *GPAI* :

- documentation permettant de bien comprendre les capacités et les limites du modèle *GPAI* ;
- preuve de conformité à la législation européenne en matière de droit d'auteur ;
- résumé détaillé de la donnée d'entraînement du modèle *GPAI*.

HUB FRANCE IA

Contributeurs

X.5 Contributeurs

Voici la liste des contributeurs, qui ont œuvré à la rédaction de ce livre blanc :

Pilotes

- **Alberto DONIN** – Société générale
- **Francesca MARTINI** – La Poste Groupe

Contributeurs

- **Benjamin BOSCH** – Société Générale
- **Cécilia DAMON** – ASNR
- **Émilie SIRVENT HEIN** – Orange
- **Geoffroy SINEGRE** – Indépendant
- **Isabelle GAVANON** – AFDIT
- **Léa DELERIS** – BNP Paribas
- **Olivia RIME** - Naaia
- **Phetdavanh SISOMBATH** – Now Brains
- **Romain SIDOBRE** - Orange
- **Valérie CHAVANNE** – LegalUp Consulting
- **Ysens DE FRANCE** – Gendarmerie nationale
- **Yann POIRIER** – Now Brains

Relecteurs

- **Bertrand CASSAR** – La Poste Groupe
- **Chloé PLEDEL** – Hub France IA
- **Françoise SOULIE** – Hub France IA

Touche finale

- **Alberto TEPOX** – Hub France IA
- **Mélanie Arnould** – Hub France IA

LA POSTE

SOCIETE GENERALE

OPERATIONNALISATION DU REGLEMENT EUROPEEN SUR L'INTELLIGENCE ARTIFICIELLE (RIA)

Septembre 2026

HUB FRANCE IA