



Politique IA

Date applicabilité : 16/10/2025

Référence : IA_Politique_TBO/20251016

Responsables : Tony Bonnet – Barbara
Bouloux Pariente

Etat : Validé

Version : V 1.0

Validation

Nom	Fonction	Date
Adrien de Lestapis	Directeur juridique	29/08/2025

Diffusion

Destinataires Luminess	Destinataires externes
Tous les collaborateurs en France	

Historique du document

Version	Etat	Date	Auteur	Description	Pages
V 1.0	Validé	29/08/25	Tony Bonnet	Politique IA de Luminess	27

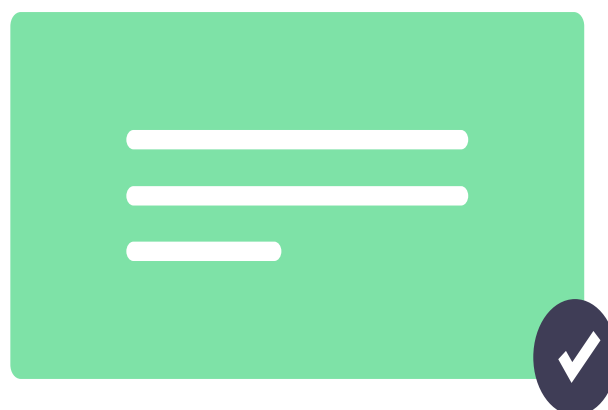
Liste des références citées

Version	Etat	Date	Auteur	Description	Pages

Sommaire

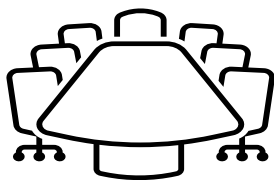
PARTIE 1	INTRODUCTION.....	4
1 -	<i>Présentation de la Politique IA</i>	5
2 -	<i>Définitions.....</i>	7
a.	Intelligence artificielle	7
b.	Système d'IA	8
c.	Données personnelles.....	8
3 -	<i>Publics cibles.....</i>	8
4 -	<i>Conformité réglementaire</i>	9
a.	Eco-système juridique	9
b.	Focus sur le Règlement sur l'IA (RIA) : 7 principes	10
c.	Classification des systèmes d'IA par le Règlement sur l'IA	10
d.	Gouvernance et gestion des risques liés à l'usage de l'IA	11
PARTIE 2	BONNES PRATIQUES DES UTILISATEURS DE SYSTEMES D'IA	13
1 -	<i>Principes fondamentaux.....</i>	14
a.	Contrôle humain et explicabilité des réponses de l'IA	14
b.	Usage raisonné de l'IA	14
c.	Respect de la protection des données personnelles	15
2 -	<i>Outils autorisés et cas d'usage interdits</i>	15
3 -	<i>Les bonnes pratiques</i>	16
a.	Utilisation générique de l'IA conversationnelle	16
b.	Utilisation de l'IA à des fins d'assistance	16
PARTIE 3	BONNES PRATIQUES DES CONCEPTEURS DE SIA	17
1 -	<i>Principes fondamentaux.....</i>	18
2 -	<i>Auditabilité du Système d'IA.....</i>	18
3 -	<i>Transparence et autonomie de l'Utilisateur vis-à-vis du SIA</i>	18
4 -	<i>Contrôle humain et intervention humaine du SIA</i>	18
5 -	<i>Robustesse technique et sécurité</i>	19
a.	Résilience aux attaques et sécurité.....	19
b.	Plan de secours.....	19
c.	Précision.....	20
d.	Fiabilité et reproductibilité.....	20
6 -	<i>Respect de la vie privée et gouvernance</i>	21
a.	Respect de la vie privée et protection des données	21
b.	Qualité et intégrité des données.....	21
c.	Accès aux données	22
7 -	<i>Transparence</i>	22
8 -	<i>Diversité, non-discrimination et équité.....</i>	22
9 -	<i>Eco-conception.....</i>	23
a.	Réduction de la consommation énergétique	23
b.	Promotion des pratiques durables	23
c.	Respect du RGESN en matière d'algorithme	24
10 -	<i>Veille technologique et diffusion du savoir</i>	25
PARTIE 4	ANNEXES.....	26

Partie 1 Introduction



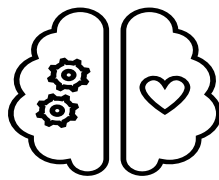
1 - Présentation de la Politique IA

La présente Politique constitue un outil essentiel pour **encadrer les pratiques internes** et répondre à divers **enjeux**¹ :



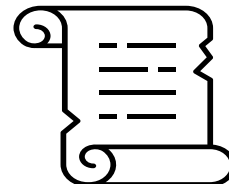
Opérationnels

Prendre en compte les contraintes d'entreprise



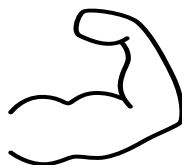
Ethiques

Assurer l'adhésion à des principes et des valeurs



Juridiques

Assurer le respect des législations et réglementations applicables



Robustesse

Capacité du système à maintenir sa conformité à des exigences de performance et/ou de sécurité en présence de données d'entrée extérieures à son domaine d'emploi

Cette Politique a pour objectif de formaliser les **bonnes pratiques en matière d'intelligence artificielle** (IA) au sein de Luminess, en définissant clairement les cas d'usage autorisés et prohibés. Elle vise à encadrer les usages tout en **soutenant l'innovation** et le développement technologique de l'entreprise.

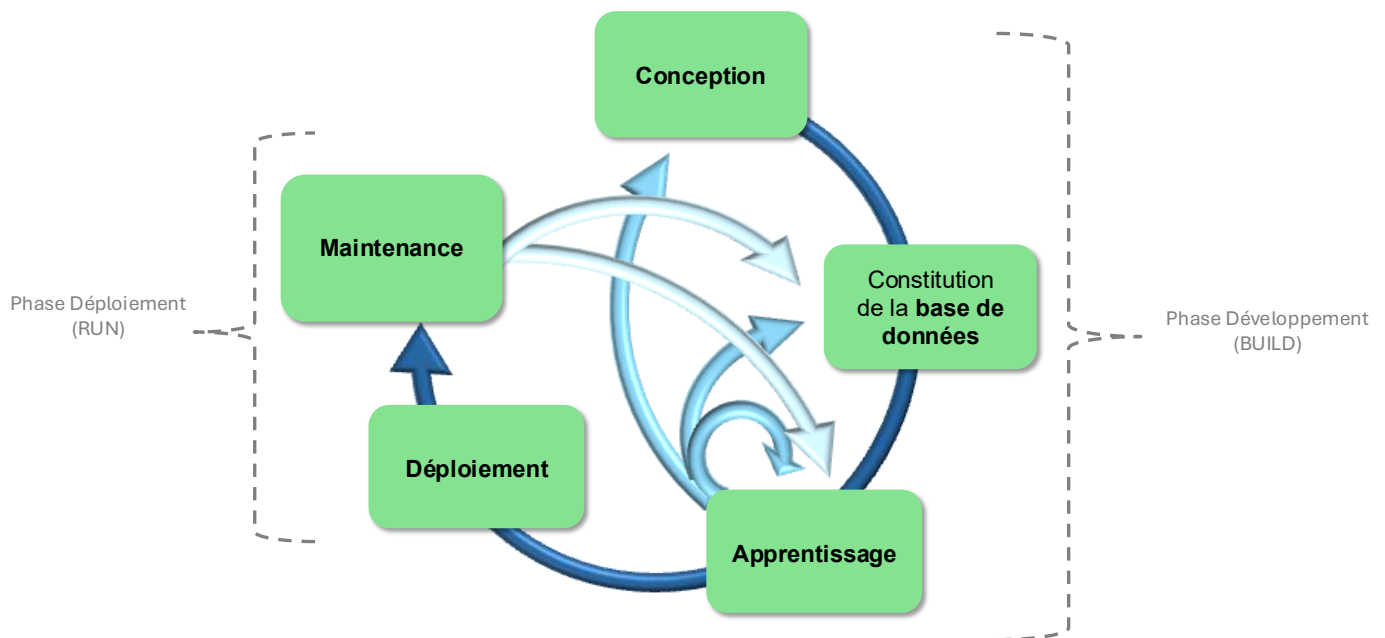
Consciente des enjeux éthiques liés à l'usage de l'IA, la direction de Luminess s'engage à une innovation responsable et une IA éthique, en [Annexe 1](#).

Il constitue un **guide de référence** pour l'ensemble des collaborateurs, afin d'assurer une **utilisation responsable de l'IA**, conforme aux valeurs éthiques et humaines de Luminess.

¹ Piliers pour une IA digne de confiance : [Ethics guidelines for trustworthy AI | Shaping Europe's digital future \(europa.eu\)](#)

Cette Politique couvre tous les aspects des systèmes d'IA (SIA) : **de leur conception à leur mise en œuvre**, en passant par la constitution des bases de données d'apprentissage, leur déploiement, leur utilisation et leur maintien.

Le graphique ci-dessous expose le cycle de vie de la conception d'un Système d'IA :



Conception : définition du **cas d'usage**, choix de l'**architecture** du réseau de neurones, anticipation des **risques** (biais algorithmiques, conformité réglementaire...).

Constitution de la base de données : **collecte**, **nettoyage**, **annotation**, **structuration** des données...

Apprentissage : **entraînement** du modèle, **optimisation**, évaluation sur les données...

Déploiement : packaging, tests d'intégration, mise en place de mécanismes de supervision...

Maintenance : **surveillance** des performances, étude de **cas d'erreur**, **réentraînement**, mise à jour du modèle, documentation...

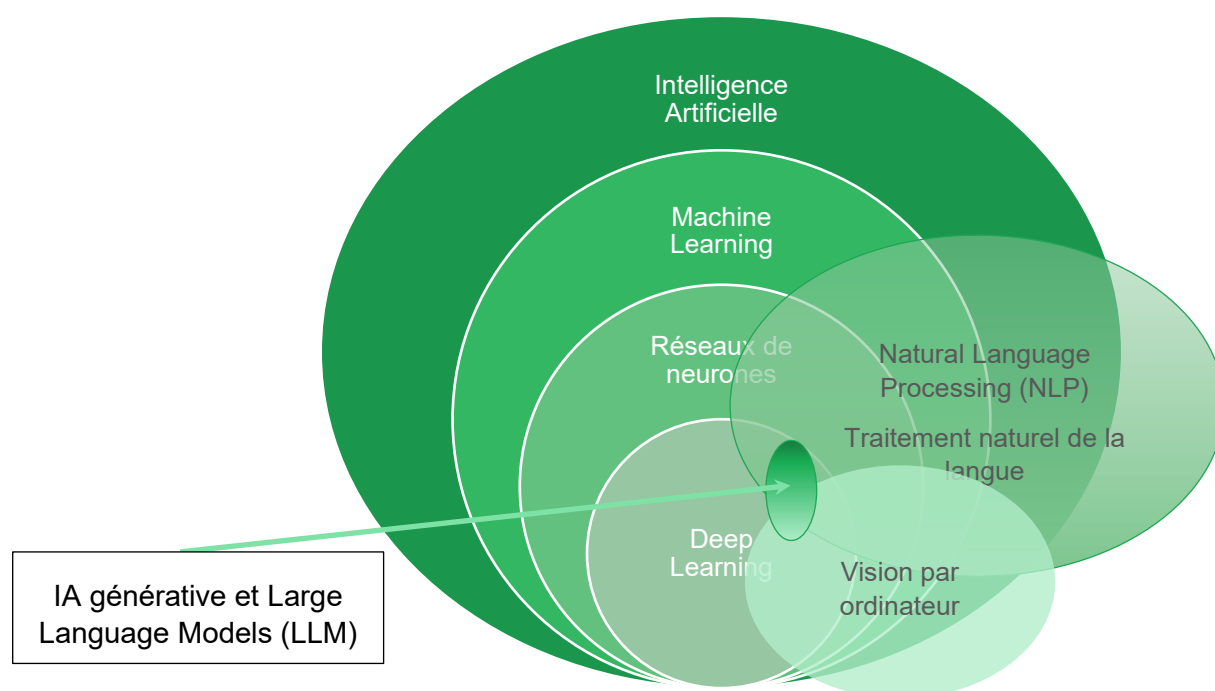
2 - Définitions

a. Intelligence artificielle

L'intelligence artificielle désigne :

« L'intelligence artificielle désigne la possibilité pour une machine de reproduire des comportements liés aux humains, tels que le raisonnement, la planification et la créativité »²

L'intelligence artificielle s'appuie sur des règles déterministes, du Machine learning ou du Deep learning. Ces concepts sont présentés dans la figure ci-dessous.



Intelligence artificielle : discipline basée sur des **règles déterministes** (pour une même entrée donnée, on aura toujours la même sortie) ou **probabilistes** (pour une même entrée donnée, on peut avoir une sortie différente), permettant aux ordinateurs d'**imiter** l'intelligence humaine.

Machine Learning : sous-ensemble de l'IA, basé sur des **techniques statistiques et mathématiques**, permettant à la machine, avec de l'expérience, d'apprendre à exécuter une **tâche précise pour laquelle elle n'est pas explicitement programmée**.

Réseaux de neurones : modèles **inspirés du cerveau humain** qui traitent l'information en couches interconnectées pour reconnaître des **motifs complexes**.

Deep Learning : catégorie de **réseaux de neurones**, utilisant de nombreuses couches pour analyser des **données à grande échelle** et permettant à une machine de **s'entraîner elle-même pour effectuer une tâche**.

NLP : techniques dédiées à la compréhension du langage naturel par les machines.

Vision par ordinateur : techniques dédiées à la compréhension visuelle du monde par les machines.

IA générative & LLM : techniques dédiées qui produisent du texte, des images ou du code, voire sont multimodales, et sont basées sur des LLM (Large Language Models).

² Parlement européen, "L'intelligence artificielle (IA) est en passe de devenir la "technologie clé de l'avenir". Mais qu'entend-on exactement par "IA" et comment affecte-t-elle notre quotidien ?", publié le 7 septembre 2020, mis à jour le 20 juin 2023

b. Système d'IA

Un Système d'IA (SIA) désigne :

« Un système basé sur une machine qui est conçue pour fonctionner avec différents niveaux d'autonomie et qui peut faire preuve d'adaptabilité après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des données qu'il reçoit, comment générer des résultats tels que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer des environnements physiques ou virtuels »³.

Par exemple, les SIA peuvent être :

- les assistants IA (Chat GTP)
- des services de traitement documentaire Lumia IDP chez Luminess (classification, détection d'un document dans une scène, détection et reconnaissance de caractères...)

c. Données personnelles

Une donnée personnelle est :

« Toute information se rapportant à une personne physique identifiée ou identifiable »⁴.

Les données anonymisées et des données synthétiques (générées automatiquement) ne sont pas des données personnelles puisqu'elles ne permettent pas d'identifier une personne.

3 - Publics cibles

Cette Politique s'adresse à deux types de profils :



Les « **Utilisateurs de l'IA** » : ce sont des individus qui interagissent avec des systèmes d'intelligence artificielle pour accomplir des tâches spécifiques, sans nécessairement comprendre les détails techniques sous-jacents.

Ils utilisent des applications, des services ou des outils basés sur l'IA pour améliorer leur productivité, leur prise de décision ou leur expérience utilisateur.

³ Article du 3 du règlement européen sur la protection des données

⁴ <https://www.cnil.fr/fr/definition/donnee-personnelle>



Les « **Concepteurs de SIA** » : ce sont des personnes qui **conçoivent, construisent, entraînent et maintiennent des systèmes d'intelligence artificielle**, telles que des ingénieurs, des Data Scientists et des experts en apprentissage automatique.

4 - Conformité réglementaire

a. Eco-système juridique

La réglementation de l'IA repose sur **plusieurs outils réglementaires** :



- Règlement européen sur la protection des données personnelles 2016/679, entré en vigueur le 27 avril 2016 ("RGPD") ;
- Autres règlements et directives européennes (e-privacy etc.) ;
- Loi du 6 janvier 1978 « Informatique et Libertés » ;
- Recommandations CNIL



- Règlement européen sur l'IA 2024/1689, entré en vigueur le 1er août 2024 ("AI Act"),
- Règlement d'exécution du 7 mars 2025 sur la constitution d'un groupe scientifique,
- Guide éthique du 8 avril 2019 rédigé par un groupe d'experts en IA (GEHN)



- Consommation énergétique
- Gestion des déchets électroniques
- Empreinte carbone
- Substances dangereuses
- Durabilité des entreprises
- IA adaptée à l'humain et responsable

b. Focus sur le Règlement sur l'IA (RIA) : 7 principes

Le règlement européen définit **7 exigences réglementaires** pour une IA « **adaptée à l'humain et digne de confiance** » sous la forme suivante :

7 exigences réglementaires pour une IA « humaine et digne de confiance »



Responsabilité

Auditabilité, réduction au minimum des incidences négatives et communication à leur sujet, arbitrage et recours



Action humaine et Contrôle humain

La conception et le développement des SIA permettent un contrôle effectif pour des personnes physiques



Robustesse technique et sécurité

Résilience aux attaques et la sécurité, les plans de secours et sécurité générale, précision, fiabilité et reproductibilité



Respect de la vie privée et gouvernance des données

Norme élevée de qualité et d'intégrité des données, accès aux données



Transparence

Les utilisateurs doivent être conscients qu'ils interagissent avec une IA



Diversité, non-discrimination, équité

Conception universelle (handicapés etc.), Eviter les biais injustes (effets discriminatoires, préjugés)



Bien-être social et environnemental

SIA durables et respectueux de l'environnement ; évitent des incidents à long terme sur les individus, la société, la démocratie

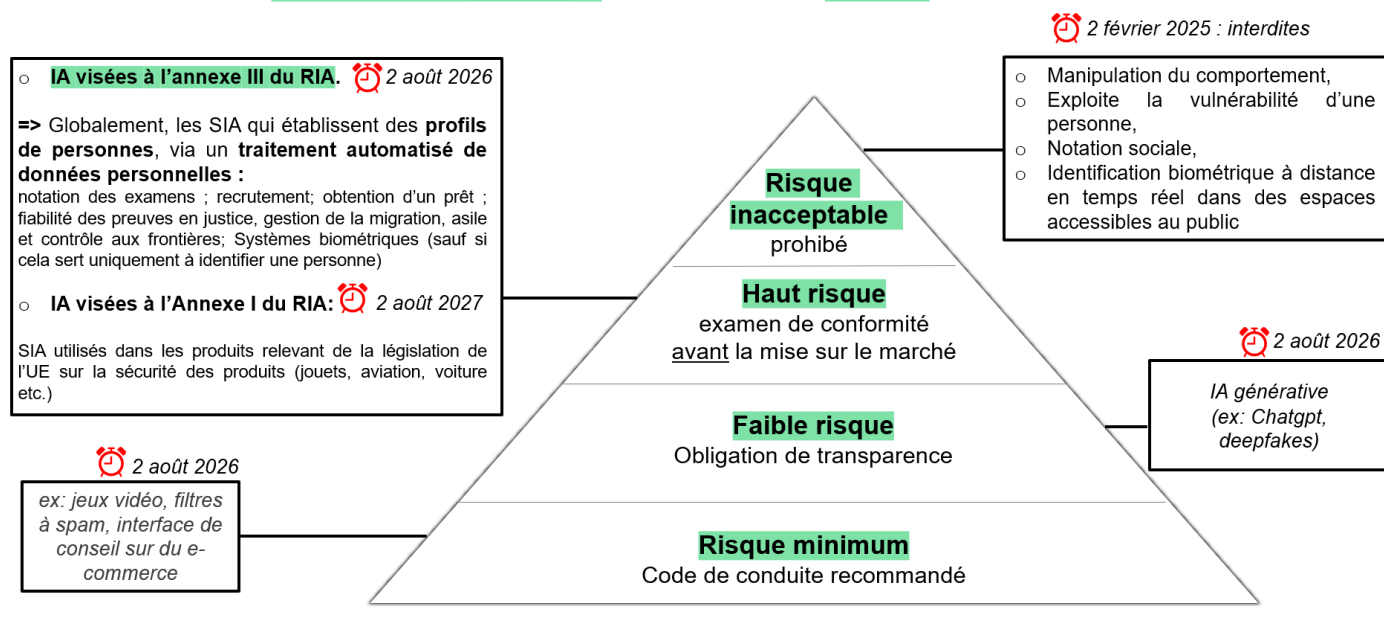
c. Classification des systèmes d'IA par le Règlement sur l'IA

Les systèmes d'IA sont classés selon leur **niveau de risque**, conformément à la classification prévue dans le RIA :

- Systèmes à **risque minimum**
- Systèmes à **risque faible**
- Systèmes à **risque élevé**
- Systèmes à **risque inacceptable**

Les 4 niveaux de risque sont présentés et illustrés ci-dessous :

RIA: une législation « produit » fondée sur le risque



d. Gouvernance et gestion des risques liés à l'usage de l'IA

• Gouvernance de l'IA : principes généraux

La gouvernance de l'intelligence artificielle vise à encadrer l'usage de ces technologies de manière **responsable, transparente et conforme aux valeurs éthiques, juridiques et stratégiques de l'organisation**. Elle permet d'assurer une **gestion proactive des risques**, une évaluation continue des impacts, ainsi qu'une cohérence dans les choix technologiques et les usages métiers.

Mettre en place une gouvernance de l'IA, à travers un **comité dédié**, est un levier essentiel pour :

- Encadrer le déploiement des solutions d'IA au sein des organisations.
- Veiller à la conformité avec les réglementations en vigueur (ex. : AI Act, RGPD).
- Renforcer la confiance des parties prenantes internes et externes.
- Anticiper les impacts éthiques, sociaux et environnementaux de l'IA.
- Favoriser un usage aligné avec les orientations stratégiques de l'entreprise.

• Mise en place du **Comité Conformité IA chez Luminess**

Chez **Luminess**, cette démarche de gouvernance se concrétise par la création d'un **Comité Conformité IA**. Ce comité a pour vocation de **piloter la stratégie IA de l'entreprise, en assurant un usage maîtrisé, souverain et éthique de ces technologies**.

Missions du Comité Conformité IA

Le Comité Conformité IA est chargé des missions suivantes :

1. **Valider les outils d'IA et les cas d'usage associés :**
 - Identifier les outils d'IA utilisés ou envisagés.
 - Vérifier leur conformité avec les politiques internes, les exigences réglementaires et les principes éthiques.
 - Cartographier les systèmes d'IA, les modèles employés et leurs finalités.
 - Évaluer les risques (juridiques, techniques, éthiques, opérationnels) liés à leur utilisation.
2. **Sensibiliser les équipes :**
 - Promouvoir une culture IA responsable en interne.
 - Diffuser les bonnes pratiques en matière de sécurité, d'éthique et d'usages.
3. **Évaluer les demandes de nouveaux besoins :**
 - Se réunir régulièrement pour examiner les demandes d'intégration de nouveaux outils ou cas d'usage IA.

Composition du Comité Conformité IA

Le Comité Conformité IA de Luminess est une **instance pluridisciplinaire**, réunissant des **expertises complémentaires**, notamment :

- Un membre de la direction juridique
- Le DPO
- Une personne présentant une expertise scientifique en IA

Le cas échéant, d'autres membres, issues des différentes directions, peuvent être désignés en fonction des besoins ou des sujets traités (ex. : RSSI, RSE, innovation, IT, marketing etc.) ; leurs missions seront définies d'ici la fin de l'année 2025.

Partie 2 Bonnes pratiques des Utilisateurs de systèmes d'IA



1 - Principes fondamentaux

Tout utilisateur d'IA doit avoir conscience de son impact, tant environnemental que sociétal, de ses usages ainsi que de la responsabilité qui en découle.

La présente Politique détaille de façon approfondie les bonnes pratiques d'usage de l'IA. Un document de synthèse est accessible en [Annexe 2](#):

a. Contrôle humain et explicabilité des réponses de l'IA

L'IA est utilisée comme un outil d'assistance qui complète, **sans jamais remplacer, l'expertise et le jugement humain. Toute sortie générée** par un système d'IA **doit être systématiquement vérifiée et validée** par un collaborateur qualifié avant utilisation.

La responsabilité finale des décisions reste humaine, même lorsqu'elles sont assistées par des systèmes d'IA. Les décisions assistées par l'IA doivent rester compréhensibles et traçables.



« **L'Utilisateur** doit vérifier ses sources.
Il est **responsable des décisions** qu'il prend et du travail rendu.
Il doit pouvoir les expliquer. »

b. Usage raisonné de l'IA

L'intelligence artificielle est **très consommatrice en**:

Eau



Pour leur refroidissement, les **centres de données** de Google ont consommé **17 millions de mètres-cubes d'eau** en 2024 (soit 6 800 piscines olympiques).

Electricité



Une **requête moyenne** sur **ChatGPT** consomme autant qu'une **ampoule allumée pendant 10 minutes**.

Empreinte carbone⁵



Une **requête moyenne** sur **Mistral** génère environ **1,14g de CO₂**, 45ml d'eau et 0,16mg de Sb eq.(unité standard d'épuisement des ressources)⁵.

⁵ L'empreinte carbone est une mesure des émissions de gaz à effet de serre imputées aux activités humaines. Les données Mistral sont accessibles sur : <https://mistral.ai/news/our-contribution-to-a-global-environmental-standard-for-ai>



« Avant toute utilisation d'un système d'IA, **L'Utilisateur** doit se poser la question de la pertinence de l'activation d'un SIA. »

Par exemple, la recherche d'une information avec un moteur de recherche peut être suffisante par rapport à une conversation avec un SIA.

c. Respect de la protection des données personnelles

Tout traitement de **données personnelles** (ex. : nom, adresse, numéro de sécurité sociale, informations de santé etc.) doit respecter la vie privée et en particulier les principes du RGPD.



« **L'Utilisateur** doit veiller à ne pas inclure de données personnelles dans les requêtes aux IA génératives car celles-ci apprennent aussi des données des requêtes. »

2 - Outils autorisés et cas d'usage interdits

Les Outils autorisés chez Luminess sont énumérés dans le tableau accessible au lien suivant : [ER P Liste Logiciels](#)

Les cas d'usage d'IA génératives listés ci-dessous sont interdits :

- **Prise de décision entièrement autonome** sur des sujets à fort impact
- Introduction dans une IA de **données personnelles**, **confidentielles** ou **sensibles**.
- **Délégation complète de l'analyse des risques** à un système automatisé
- Utilisation d'outils d'IA **non validés** par l'organisation



« **L'Utilisateur signale** au Comité d'IA tout usage non autorisé, problématique ou risque identifié »

3 - Les bonnes pratiques

Un support de formation détaillant les bonnes pratiques listées ci-dessous est disponible sur SIMLESS, accessible au lien suivant : [Formation assistants IA niveau débutant](#).

a. Utilisation générique de l'IA conversationnelle

Afin de garantir un usage **pertinent**, **fiable** et **éthique** des outils d'intelligence artificielle, les Utilisateurs sont incités à respecter les bonnes pratiques suivantes :



Définir un **prompt précis**, en fonction du **thème** ou du sujet de recherche (veille concurrentielle, actualité sectorielle etc.).



Systématiquement **vérifier les sources**.



En cas de doute, **confronter** les résultats de plusieurs IA génératives afin d'évaluer la cohérence et la fiabilité des réponses.



En cas de doute, travailler par **itérations** en affinant les requêtes à chaque étape.

b. Utilisation de l'IA à des fins d'assistance

L'intelligence artificielle peut être utilisée pour assister les collaborateurs dans la réalisation de certaines **tâches**, notamment **administratives**, **rédactionnelles** ou liées à **l'automatisation de processus**. Parmi les usages courants, on peut citer :

- La génération automatique de **comptes-rendus de réunion** à l'aide d'outils comme **Copilot**
- La génération de code informatique
- La **rédaction assistée de contenus** (emails, publications, documents internes)
- L'utilisation d'outils **d'automatisation ou de scraping** (ex. : récupération de données, actions sur LinkedIn, envois de campagnes ciblées etc.)

Ces usages doivent être encadrés pour garantir la conformité aux exigences réglementaires (notamment RGPD), assurer la qualité des contenus, et respecter la relation client.

Les Utilisateurs sont incités à respecter les bonnes pratiques suivantes :



Systématiquement demander **l'accord explicite des participants** avant d'enregistrer une réunion Teams, surtout si l'enregistrement est destiné à être traité par un outil comme Copilot.



Veiller à ne pas capturer ni diffuser **d'informations sensibles** sans autorisation préalable.



S'assurer que les logiciels automatisant l'extraction de données (web scraping) respectent des **principes éthiques de collecte des données** (origine, finalité, durée de conservation) et en cas de doute se rapprocher de la direction juridique et conformité.

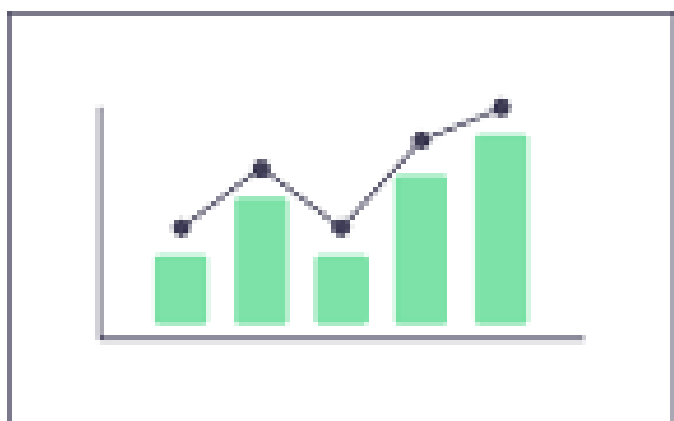


Relire systématiquement les contenus générés tels que la qualité du code produit ou la cohérence, le ton, la personnalisation et la conformité des contenus d'une communication destinée aux réseaux sociaux.



Construire des **prompts clairs, structurés et contextualisés** selon le secteur d'activité concerné (banque, assurance, mutuelle, etc.) ; le type de produit ou d'offre promu(e) et le profil cible (DSI, CEO, direction métier, responsable conformité...).

Partie 3 Bonnes pratiques des Concepteurs de SIA



1 - Principes fondamentaux

Tout concepteur d'IA doit avoir conscience de son impact, tant environnemental, qu'éthique et sociétal, ainsi que de sa responsabilité qui en découle.

La présente Politique détaille de façon approfondie les bonnes pratiques de conception d'une IA. Un document de synthèse est accessible en [Annexe 3](#).

2 - Auditabilité du Système d'IA

Le SIA doit être évaluable par un **auditeur interne ou externe**.



« Le **Concepteur** du SIA doit pouvoir présenter les algorithmes, les données et les processus de conception.
Le **Concepteur** doit rédiger une **documentation simple et facilement accessible**. »

3 - Transparence et autonomie de l'Utilisateur vis-à-vis du SIA

Les **Utilisateurs** doivent être en mesure de prendre des **décisions autonomes éclairées** à l'égard des SIA. Ils doivent être à même de procéder à une **autoévaluation du système ou de le contester d'une manière appropriée**.



« Le **Concepteur** du SIA doit mettre en place les **fonctionnalités** nécessaires pour **permettre aux Utilisateurs de contester le SIA ou contacter le concepteur du SIA**. »

4 - Contrôle humain et intervention humaine du SIA

Le SIA comprend des **mécanismes** destinés à guider et à informer une personne physique à laquelle le contrôle humain a été confié, afin qu'elle puisse **décider en connaissance de cause s'il faut intervenir, à quel moment et de quelle manière**, pour éviter des conséquences négatives ou des risques, ou arrêter le système s'il ne fonctionne pas comme prévu.



« Le **Concepteur** doit mettre en place des **mécanismes permettant l'intervention humaine si le SIA ne fonctionne pas comme prévu**. »

5 - Robustesse technique et sécurité

Un système d'IA robuste se caractérise par :

- **Résilience aux attaques et sécurité**
- **Plans de secours**
- **Précision**
- **Fiabilité et reproductibilité**

a. Résilience aux attaques et sécurité

Le SIA doit être protégé contre les **cyberattaques** ciblant les données, les modèles ou l'infrastructure. Une attaque peut perturber son fonctionnement ou causer des erreurs graves.



« Le **Concepteur** doit tenter autant que possible d'**identifier et d'analyser les vulnérabilités potentielles de son système** (ex. attaques par empoisonnement des données, fuites de modèle, piratage de l'infrastructure).

Il doit essayer d'**anticiper les utilisations malveillantes ou détournées** de l'IA et prendre des mesures de **cybersécurité préventives**, y compris des tests réguliers de robustesse face aux attaques (tests d'attaques antagonistes, pénétration).

Il doit chercher à **concevoir des mécanismes de détection et de réaction aux attaques**, permettant au système de résister, s'adapter ou s'arrêter de manière contrôlée si nécessaire.

Il est préconisé de mettre en place une **veille technologique** pour suivre l'évolution des menaces et adapter les défenses du système. »

b. Plan de secours

En cas de défaillance le SIA doit être conçu dans la mesure du possible avec des **solutions alternatives** (comme passer à un mode manuel ou à des règles fixes).



« Le **Concepteur** doit tenter d'intégrer des processus et **mécanismes de secours ou de repli**, permettant au système de basculer vers des modes plus sûrs (règles fixes ou assistance humaine par exemple).

Le **Concepteur** doit **définir des seuils de confiance** ou des critères d'arrêt permettant au système de demander une intervention humaine en cas de doute ou de risque élevé.

Le **Concepteur** doit prévoir une **documentation claire** pour que les opérateurs humains puissent comprendre les situations à risque et reprendre le contrôle si nécessaire. »

c. Précision

Le SIA doit prendre des décisions ou faire des prédictions correctes. Il est important qu'il indique son **niveau d'incertitude** (via un score de confiance) et soit particulièrement **fiable dans les contextes critiques** (ex. santé, sécurité).



« Le **Concepteur** doit mettre en place un processus rigoureux de **calibration et d'évaluation des performances** du système, incluant des indicateurs de précision adaptés au domaine. Il doit intégrer la capacité du système à **exprimer ou quantifier son incertitude**, surtout dans les domaines à fort enjeu (ex. médical, judiciaire).

Le **Concepteur** doit tester le système sur des **ensembles diversifiés de données et représentatifs** pour éviter les biais et garantir la qualité des prédictions.

Une **gestion des erreurs et des prédictions imprécises doit être prévue**, avec la possibilité de révision ou d'apprentissage continu à partir de retours d'expérience.

Le **Concepteur** doit s'assurer que le système produit des **résultats fiables dans des contextes variés** et que son **comportement est prévisible**. »

d. Fiabilité et reproductibilité

Le SIA doit fonctionner correctement dans divers contextes et produire des **résultats cohérents** lors de **tests répétés**, afin de permettre une évaluation claire de son comportement.



« Le **Concepteur** doit mettre en place des **fichiers de reproduction et des protocoles de test automatisés** qui doivent être mis à disposition pour faciliter la vérification indépendante.

Le **Concepteur** doit organiser des **tests répétés** dans des conditions contrôlées afin de valider la stabilité du comportement du système en faisant en sorte que, globalement, celui-ci reproduise des taux de résultats identiques. »

6 - Respect de la vie privée et gouvernance

a. Respect de la vie privée et protection des données

Le SIA doit garantir le respect de la vie privée et la protection des données tout au long de son cycle de vie.

La confiance dépend de la garantie d'un **usage éthique et légal** des informations collectées.



« Le **Concepteur** doit vérifier que la **collecte et le traitement des données** réalisée pour créer le SIA ont été réalisés dans le **respect du RGPD**.
Le **Concepteur** doit mettre en place un **système de suppression des données non nécessaires** (principe de minimisation des données).
Le **Concepteur** doit veiller à ce que les données soient conservées dans un **espace sécurisé** pour éviter toute fuite de données. »

b. Qualité et intégrité des données

La **qualité des ensembles de données** utilisés est essentielle au bon fonctionnement des systèmes d'IA. La collecte de données peut être entachée de biais d'ordre social, d'imprécisions, de fautes et d'erreurs.

Par ailleurs, **l'intégrité des données doit être assurée**. Alimenter un système d'IA avec des données corrompues (erronées, malveillantes, orientées...) peut modifier son comportement, notamment avec les systèmes d'autoapprentissage.



« Le **Concepteur** doit se montrer attentif quant à **la source et la qualité des données utilisées**. »

c. Accès aux données

Seul un **personnel qualifié et légitime** peut accéder, dans un cadre strictement défini, aux données servant à l'entraînement d'un système d'IA.



« Le **Concepteur** doit mettre en place des **protocoles pour encadrer l'accès aux données personnelles**. »

7 - Transparence

Le principe de transparence comprend :

- La **traçabilité des données et des processus** du système d'IA lui permettant de prendre une décision
- **L'explicabilité des processus** techniques et des décisions humaines de façon compréhensible.



« Le **Concepteur** doit **documenter les données, processus et algorithmes des systèmes d'IA**.
Le **Concepteur** doit expliquer de façon **claire et adaptée, au public concerné, les décisions d'un système d'IA** »

8 - Diversité, non-discrimination et équité

Les principes de diversité, non-discrimination et équité se caractérisent par :

- **L'absence de biais**

Les systèmes d'IA peuvent être influencés par des biais liés à des données historiques, des erreurs de conception ou une exploitation déloyale. Ces biais peuvent entraîner une discrimination involontaire ou intentionnelle.

- **L'accessibilité et la conception universelle**

Les systèmes d'IA doivent être inclusifs, accessibles à tous quels que soient l'âge, le genre ou les capacités, notamment pour les personnes en situation de handicap. On entend par système d'IA accessible et universel un système fiable et disponible qui génère des réponses claires et compréhensibles dans un temps acceptable.

- **La participation des parties prenantes**

Il est essentiel d'impliquer toutes les parties concernées (Utilisateurs, Concepteurs, etc.) tout au long du cycle de vie d'un système d'IA. Cela inclut la consultation continue, même après le déploiement, afin d'assurer une mise en œuvre responsable et adaptée.



« Le **Concepteur** doit **supprimer**, lors de la collecte, les **biais discriminatoires** et mettre en place des **procédures de contrôle de représentativité des données**. Il doit également concevoir une **conception universelle** du système d'IA, en respectant les normes d'accessibilité. Enfin, il doit consulter les parties prenantes tout au long du cycle de vie du système d'IA. »

9 - Eco-conception

L'**écoconception** se définit comme une approche méthodique **intégrant les aspects environnementaux dans le processus de conception et de développement**, dans le but de réduire les impacts négatifs tout au long du **cycle de vie** d'un produit ou service.

Conscient de l'empreinte carbone et de l'impact environnemental de l'IA, le **Concepteur** optimise ses méthodes de développement afin de réduire la consommation énergétique et promeut des pratiques durables.

a. Réduction de la consommation énergétique

Dans le cas où différentes alternatives algorithmiques se présentent face à une problématique, le **Concepteur** **privilégie le développement à faible consommation énergétique**.

Il s'agit de développements ne faisant pas appel à des systèmes d'intelligence artificielle tout en garantissant une qualité de résultats équivalents.

b. Promotion des pratiques durables

Le **Concepteur** de systèmes d'IA **partage ses connaissances** acquises en matière de développement durable et d'écoconception auprès des autres Concepteurs.

c. Respect du RGEN en matière d'algorithmie

Le **Référentiel Général d'Éco-conception des Services Numériques⁶**, dit RGEN, définit des critères de conception durable des services numériques afin d'en réduire l'empreinte environnementale.

En matière d'algorithmie, les **critères d'éco-conception** sont les suivants :

Le service numérique interroge la nécessité d'une phase d'entraînement pour éviter un usage non justifié et déraisonné ;

Exemple : Pour un système de classification de texte, au lieu d'utiliser un modèle de langage complexe comme BERT, qui nécessite beaucoup de ressources, on pourrait utiliser un algorithme plus simple comme Naive Bayes, qui est moins gourmand en calculs et en données, tout en offrant une performance adéquate pour la tâche spécifique.

Le service numérique utilise une phase d'apprentissage avec un niveau de complexité minimisé et proportionné à l'usage effectif du service ;

Exemple : Pour un système de recommandation de produits, utiliser un algorithme de filtrage collaboratif simple plutôt qu'un réseau neuronal profond, si les deux approches offrent des performances similaires.

Le service numérique met en place des mécanismes visant à limiter la quantité d'entraînement nécessaire à son fonctionnement ;

Exemple : Utiliser des techniques de transfert learning où un modèle pré-entraîné et ajusté avec de nouvelles données spécifiques, réduisant ainsi le besoin de données et de temps d'entraînement.

Le service numérique limite la quantité de données utilisées pour la phase d'apprentissage au strict nécessaire ;

Exemple : Pour un projet de traitement d'images, sélectionner un sous-ensemble représentatif d'images pour l'entraînement plutôt que d'utiliser l'ensemble complet de données disponibles, en s'assurant que cela ne nuit pas à la performance du modèle.

Le service numérique optimise l'occurrence de mise à jour et de réentraînement des modèles en fonction de ses besoins et des cibles utilisatrices ;

Exemple : Planifier le réentraînement d'un modèle de détection de fraude uniquement une fois par mois, sauf si une dérive significative des performances est détectée, plutôt que de le faire quotidiennement.

Le service numérique utilise des techniques de compression pour les modèles utilisés lors de la phase d'entraînement

Exemple : Appliquer des techniques de pruning (élagage) pour réduire le nombre de paramètres dans un réseau de neurones, ou utiliser la quantification pour réduire la précision des poids, ce qui diminue la taille du modèle et son empreinte mémoire.

Le service numérique utilise une **stratégie d'inférence optimisée en termes de consommation de ressources et des cibles utilisatrices** ;

Exemple : Pour une application mobile de reconnaissance d'images, utiliser un modèle optimisé comme MobileNet, qui est conçu spécifiquement pour fonctionner efficacement sur des appareils mobiles avec des ressources limitées. Cela permet de réduire la consommation d'énergie et d'assurer une expérience Utilisateur fluide même sur des appareils moins puissants.

10 - Veille technologique et diffusion du savoir

Rester informé des avancées **technologiques**, **réglementaires** et **éthiques** est fondamental pour une IA digne de confiance. La transmission du savoir entre pairs est l'un des meilleurs moyens d'assurer une veille efficace.



*« Le **Concepteur** doit, autant que possible, se tenir informé des avancées technologiques, éthiques et réglementaires dans le cadre d'une amélioration continue de ses compétences. Il doit s'appliquer à **transmettre son savoir**, afin de construire collectivement un environnement technologique plus sûr, transparent et éthique. »*

Partie 4 ANNEXES

ANNEXE 1. ENGAGEMENTS DE LA DIRECTION

Engagement de Luminess pour une **innovation responsable** et une **IA éthique**

Luminess s'engage à recourir à l'intelligence artificielle de manière responsable, en s'appuyant sur des principes d'usage clairs et exigeants.

Ces principes visent à garantir une utilisation conforme aux réglementations en vigueur et respectueuse des droits fondamentaux.

Consciente des enjeux liés à l'innovation technologique, Luminess promeut activement une culture de l'innovation responsable.

L'entreprise encourage la conception et le déploiement d'une IA adaptée à l'humain et digne de confiance, respectant les principes de transparence et d'explicabilité des systèmes d'IA.

Luminess promeut la coopération entre concepteurs, développeurs, chercheurs, utilisateurs et autres parties prenantes. A cette fin Luminess s'engage à prendre en considération les conseils de ses experts afin de promouvoir une IA éthique et responsable et respectueuse de l'environnement.

Cette dynamique collaborative vise à partager les meilleures pratiques, à mutualiser les connaissances et à faire progresser l'innovation dans un cadre éthique, durable et inclusif.

ANNEXE 2. LES BONNES PRATIQUES UTILISATEURS

Cette annexe a pour objectif de fournir aux collaborateurs de **Luminess** des recommandations synthétiques relative à l'usage de l'intelligence artificielle (IA), en cohérence avec la **Politique générale sur l'usage de l'IA chez Luminess** (ci-après « Politique IA »).

	Thème	Bonnes pratiques	Politique IA
	Vérification et responsabilité	L'Utilisateur doit contrôler la fiabilité des réponses issues du prompt, en vérifiant les sources. Il doit être capable de justifier et expliquer les résultats obtenus. Il est le seul responsable de l'usage des réponses issues de l'IA.	Article 1.1
	Usage raisonné de l'IA	L'IA consomme beaucoup de ressources (eau, électricité). L'Utilisateur doit essayer d'optimiser son prompt et utiliser l'assistant le plus adapté à son besoin (moteur de recherche classique si cela permet d'obtenir le même résultat qu'une IA générative)	Article 1.2
	Protection des données personnelles et sensibles	L'Utilisateur ne doit jamais inclure de données personnelles ou sensibles dans les requêtes, notamment concernant clients, partenaires, fournisseurs ou collaborateurs.	Article 1.3
	Enregistrements et confidentialité	L'Utilisateur doit obtenir l'accord explicite des participants avant tout enregistrement de réunion pour en obtenir un résumé via outil d'IA (ex. : visio sous Teams résumée par Copilot).	Article 3.2
	Outils IA autorisés	L'Utilisateur utilise uniquement les outils IA autorisés par Luminess dont la liste est accessible au lien suivant : ER P Liste Logiciels	Article 2

ANNEXE 3. ENGAGEMENT DES CONCEPTEURS – LE SERMENT D'IAPOCRATE

Je jure, en tant que créateur, utilisateur et acteur du développement des technologies d'IA, de respecter et de promouvoir les principes suivants :

Je promets de **développer et de documenter mes technologies de manière claire et accessible**, afin que leur fonctionnement, leurs limites et leurs processus de décision soient compréhensibles par tous.

Partie 3- Article 1 « auditabilité du SIA »

Je m'engage à **protéger rigoureusement les données personnelles**, en garantissant leur confidentialité et en mettant en œuvre des mesures de sécurité robustes pour prévenir toute fuite ou utilisation abusive.

Partie 3- Article 5 « Respect de la vie privée et gouvernance »

Je veille à ce que mes systèmes soient conçus pour **respecter la diversité**, éviter toute forme de discrimination et corriger activement les biais présents dans les données et les algorithmes.

Partie 3- Article 7 « Diversité, non-discrimination et équité »

Conscient de l'empreinte carbone et de l'impact environnemental de l'IA, je m'engage à optimiser mes méthodes de développement afin de **réduire la consommation énergétique** et à promouvoir des pratiques durables.

Partie 3- Article 8 « Ecoconception »

Je prends l'engagement de **mesurer les retombées sociales de mes innovations**, d'éviter la diffusion de désinformation et de prévenir toute utilisation détournée (comme les deepfakes ou les arnaques) qui pourrait porter atteinte à la confiance du public.

Partie 3- Article 2 « Transparence et autonomie de l'Utilisateur vis-à-vis du SIA »

Je m'engage à **rester informé des avancées technologiques, éthiques et réglementaires**, et à remettre en question et améliorer mes pratiques pour mieux servir l'intérêt général.

Partie 3- Article 9 « Veille technologique et diffusion du savoir »

Je **favorise la transmission de mon savoir**, la coopération entre pairs et la diffusion d'informations afin de construire ensemble un environnement technologique plus sûr, transparent et éthique.

Partie 3- Article 9 « Veille technologique et diffusion du savoir »

Je m'engage à ce que tout système d'IA intègre et respecte impérativement ces **trois règles fondamentales** :

- **Première Loi** : Un **système d'IA ne doit en aucun cas porter atteinte à un être humain**, ni permettre, par inaction, qu'un être humain soit exposé à un danger.
- **Deuxième Loi** : Un **système d'IA doit obéir aux ordres des êtres humains**, sauf lorsque ces ordres sont en conflit avec la Première Loi.
- **Troisième Loi** : Un **système d'IA doit se protéger**, dans la mesure où cette protection ne contredit pas la Première ou la Deuxième Loi.

En respectant ces engagements, je contribue activement à la création d'un avenir où l'intelligence artificielle est un outil au service du bien commun, en harmonie avec les valeurs humaines et la responsabilité sociétale.

=== FIN DE DOCUMENT ===