

Guide

Encadrer l'usage de l'IA au sein des associations et fondations

Gouvernance de l'intelligence artificielle et intérêt général :
un équilibre entre opportunités et responsabilités

Sommaire

Introduction	3
Edito de France générosités	4
Edito de Don en Confiance	5

6

Étape 1 Quelles opportunités de l'IA pour le secteur de la générosité ?

1. Qu'est ce que l'IA ?	7
2. L'usage de l'IA est-il réglementé ?	8
3. Quelles opportunités pour quels usages ?	12
4. Comment sélectionner les outils d'intelligence artificielle conformes ?	13

17

Étape 2 Cartographier les risques et évaluer la pertinence du recours à l'IA

1. Quels sont les risques intrinsèques à l'IA ?	18
2. Comment identifier les risques propres son association ou sa fondation ?	20
3. Comment évaluer le bénéfice-risque à l'utilisation de l'IA ?	23

24

Étape 3 Comment mettre en place une gouvernance de l'IA ?

1. Comment définir et répartir les responsabilités ?	25
2. Comment construire un cadre responsable et éthique de l'usage de l'IA ?	26
3. Exemples de bonnes pratiques à inclure dans sa charte éthique ou sa politique d'usage dédiée à l'IA	28
4. Comment intégrer et renouveler les procédures internes de l'OSBL pour un usage contrôlé de l'IA ?	31
5. Comment informer, sensibiliser et former les équipes opérationnelles à un usage responsable de l'IA ?	34

Remerciements, liste des abréviations et crédits	35
--	----

Introduction

Si l'intelligence artificielle, notamment générative (IA et IAG), représente une opportunité majeure pour les organismes sans but lucratif (OSBL), cette technologie soulève d'importantes questions techniques, juridiques et éthiques. Comment concilier innovation et respect des valeurs fondamentales ? Quels risques spécifiques les OSBL doivent-ils prévenir ? Comment garantir une utilisation responsable de cette technologie, alignée avec leur mission sociale ? Quelle gouvernance de l'IA adopter ?

Ce guide s'adresse aux professionnels des associations et fondations qui souhaitent définir une politique interne d'usage de l'IA adaptée à leur structure.

Il a pour objectif de donner des repères pour avancer en trois étapes dans la mise en place d'un système d'intelligence artificielle, en s'appuyant sur les réglementations en vigueur et les bonnes pratiques du secteur de la générosité :

- **Étape 1 : Exploration.** Quelles opportunités de l'IA pour le secteur de la générosité ?
- **Étape 2 : Analyse des risques.** Comment cartographier les risques et évaluer la pertinence du recours à l'IA ?
- **Étape 3 : Construction d'un cadre sécurisé.** Comment mettre en place une gouvernance de l'IA ?

Ce guide est conçu pour être pratique et modulaire : chaque partie peut être explorée indépendamment selon les besoins et la maturité de l'OSBL (découverte, réflexion stratégique ou déploiement opérationnel).

Avertissements :

Ce guide ne prétend pas couvrir de manière exhaustive l'ensemble des enjeux liés à l'intelligence artificielle. Son objectif est d'**offrir des pistes de réflexion et des bonnes pratiques** pour accompagner les organisations d'intérêt général dans une démarche responsable et adaptée à leurs besoins. **Les technologies d'IA évoluant très rapidement, il est à ce titre indispensable de réaliser une veille régulière**, notamment législative. Rester informé des avancées technologiques, des nouvelles réglementations et des besoins changeants de son organisation est indispensable pour **adapter ses pratiques et cadres internes**.

À la date de sa publication, les principes présentés dans ce guide ne constituent pas des règles ou exigences déontologiques du référentiel Don en Confiance. Ce document a pour objectif de proposer des repères et des bonnes pratiques destinés à accompagner les organismes d'intérêt général dans leurs réflexions, en cohérence avec les principes portés par la charte du Don en Confiance.

Édito de France générosités

L'intelligence artificielle, tout le monde en parle et de plus en plus d'associations et de fondations européennes s'y mettent. L'étude *Non-profit Pulse*¹ publiée fin 2025 par le réseau européen « European Fundraising Association » qui rassemble les données de 751 organisations à travers quatre pays, dont la France, démontre que l'IA s'est solidement implantée dans le secteur non lucratif. Près de la moitié (48 %) des organisations à but non lucratif utilisent désormais l'IA, soit une augmentation significative par rapport aux 13 % de 2024, et 56 % se disent ouvertes à son adoption. Celle-ci varie à travers l'Europe. En France, 36 % des organisations à but non lucratif utilisent l'IA, contre 78 % aux Pays-Bas.

Cependant, près de la moitié des organisations s'inquiète des risques liés à la confidentialité et à la sécurité des données, un tiers s'inquiète de la suppression d'emplois ou de la perte de compétences, et une sur cinq souligne des problèmes liés à la précision ou à l'éthique.

En France, nous avons choisi avec Don en Confiance de poser la première pierre de l'édifice collectif d'encadrement de l'usage de l'IA avec ce guide conçu comme un outil modulable et appropriable par chaque organisation afin de mieux comprendre les enjeux, se poser les bonnes questions et construire sa propre gouvernance interne pour un usage responsable et éthique de l'IA.

Notre secteur, face au vertige technologique, a besoin de collectif pour mutualiser les ressources, partager les savoirs et les cas d'usage, expérimenter pour mieux comprendre et privilégier des solutions accessibles et frugales.

Laurence Lepetit

Déléguée générale de France générosités

(1) European Fundraising Association (EFA), [Europe's nonprofits face challenges head on with strategy changes & AI adoption at pace](#), 8 décembre 2025

Édito de Don en Confiance

L'intelligence artificielle s'installe rapidement dans les outils et les pratiques des organisations d'intérêt général. Pour les associations et fondations, la question n'est plus de savoir si l'IA est déjà là, mais comment l'utiliser sans fragiliser ce qui fonde leur action : la confiance.

Chez Don en Confiance, nous sommes convaincus que l'innovation technologique ne peut être dissociée d'une exigence éthique forte. Les organismes sans but lucratif agissent auprès de publics parfois vulnérables, mobilisent des données sensibles et reposent sur une relation de confiance avec leurs donateurs, bénévoles et partenaires. Si l'IA peut constituer un levier d'efficacité, elle comporte aussi des risques réels : atteintes aux données personnelles, biais algorithmiques, opacité des décisions ou perte de contrôle humain.

Ce guide a été conçu comme un outil de cadrage. Il propose des repères concrets pour comprendre les enjeux de l'IA, identifier les usages pertinents, évaluer les risques et mettre en place une gouvernance adaptée. Il invite à replacer l'IA à sa juste place : celle d'un outil au service du projet associatif.

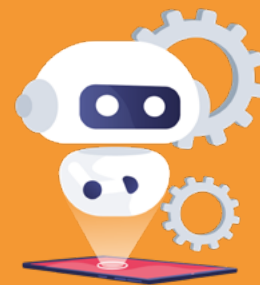
Fruit d'un travail conjoint entre les équipes de France générosités et de Don en Confiance, ce guide illustre la complémentarité de nos expertises et une conviction partagée : face à des transformations aussi structurantes que l'intelligence artificielle, les organisations de l'intérêt général ont besoin de repères communs, construits collectivement.

Encadrer l'usage de l'IA, ce n'est pas freiner l'innovation. C'est en créer les conditions durables et maîtrisées, compatibles avec les exigences de l'intérêt général, en faisant de la confiance un principe d'action, y compris à l'ère de l'intelligence artificielle.

Rachel Guez

Déléguée générale de Don en Confiance

Étape 1



Quelles opportunités de l'IA pour le secteur de la générosité ?

L'intelligence artificielle s'impose aujourd'hui comme un levier d'innovation pour tous les secteurs d'activité, y compris celui de la générosité et du milieu associatif. Cependant, avant d'adopter cette technologie, il est essentiel de s'interroger : **cette technologie répond-elle vraiment aux besoins, valeurs et contraintes de l'OSBL ?**

La première étape de la mise en place d'un système d'intelligence artificielle consiste à :

- **comprendre ses mécanismes pour en saisir les possibilités réelles**, au-delà des idées reçues
- **intégrer les contraintes réglementaires** afin de garantir une utilisation éthique et respectueuse du cadre légal
- **explorer les opportunités concrètes** que l'IA peut offrir aux organisations d'intérêt général

1. Qu'est ce que l'IA ?

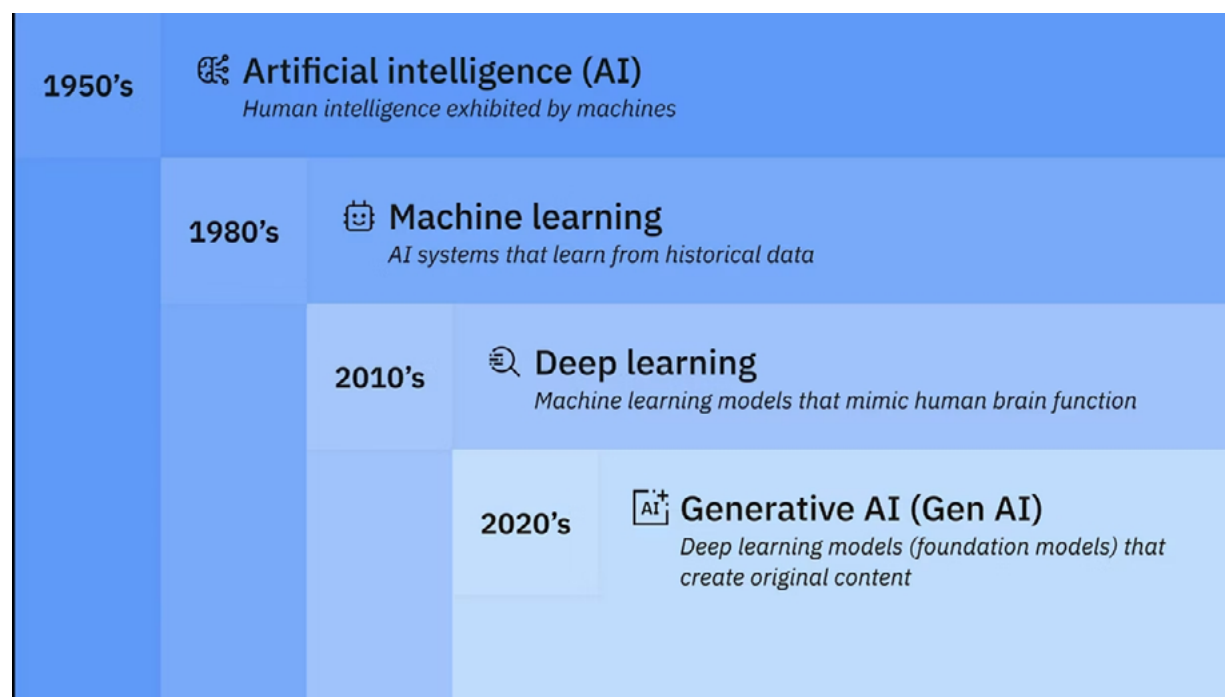
L'intelligence artificielle désigne un ensemble de technologies utilisant les données, qu'elles soient textuelles, audio ou vidéo. L'IA vise à créer des systèmes, des machines ou des programmes capables de simuler l'intelligence humaine pour réaliser des tâches qui nécessitent habituellement des capacités cognitives, telles que l'apprentissage, le raisonnement, la résolution de problèmes, la perception et la prise de décision. **Il n'y a pas une intelligence artificielle mais des intelligences artificielles** qui peuvent être combinées pour arriver à un résultat attendu.

Les avancées récentes sont largement dues à l'évolution de trois sous-domaines spécifiques de l'IA :

- **Machine Learning²** (apprentissage automatique) : c'est la méthode la plus courante de mise en œuvre

de l'IA. Elle permet aux systèmes d'apprendre et de s'améliorer à partir de données, sans être explicitement programmés pour chaque tâche. Au lieu de suivre un ensemble rigide de règles, la machine identifie des motifs et des corrélations dans les données.

- **Deep Learning³** (apprentissage profond) : c'est un sous-ensemble du Machine Learning qui utilise des réseaux complexes composés de plusieurs couches (d'où le terme «profond»). Ces modèles sont particulièrement efficaces pour les tâches de reconnaissance d'images, de parole et de traitement du langage naturel (NLP).
- **Data Science⁴** (science des données) : cette technologie utilise des méthodes scientifiques, des processus, des algorithmes et des systèmes pour extraire des connaissances à partir des données, qui sont la matière première indispensable au fonctionnement de l'IA.



Source : IBM - [Liens entre intelligence artificielle, machine learning, apprentissage profond et IA générative.](#)

(2) Commission nationale de l'informatique et des libertés (CNIL); [Glossaire](#)

(3) Ibid.

(4) Banque des Territoires, [Glossaire des projets numériques, data et IA](#)

À noter

L'entraînement est le processus de l'apprentissage automatique pendant lequel le système d'intelligence artificielle (SIA) construit un modèle à partir de données⁵. Autrement dit, le SIA s'entraîne sur un jeu de données pour effectuer la tâche attendue de lui.

Une attention particulière doit être portée aux données utilisées lors de la phase d'entraînement (texte, sons, images, listes, etc.). Cf page 14 - La sécurité et la confidentialité des données sont-elles garanties ?



Pour aller plus loin

- Glossaire des différents termes de l'IA générative sur le site de l'initiative [CaféIA](#) du Conseil National du Numérique.
- Rubrique ["Qu'est-ce que l'IA ?"](#) sur ce même site.

Concrètement, les applications sont aujourd'hui multiples et évoluent en permanence. Les exemples plus courants peuvent être cités :

- **L'automatisation** : remplacement des tâches répétitives ou chronophages pour gagner en efficacité et sécuriser des processus.
- **L'analyse et la prédiction** : traitement rapide d'énormes volumes de données pour dégager des tendances et faire des prévisions plus précises.

- **L'amélioration de la prise de décision** : fournir des analyses et des recommandations basées sur des données.
- **La création de contenus (IA générative⁶)** : il s'agit de l'application la plus répandue parmi le grand public. Elle est capable de créer de nouveaux textes, images, codes, sons, vidéos, etc. à partir de consignes données (prompt⁷).

Il est important de noter que **les applications IA s'insèrent de plus en plus dans les outils et logiciels professionnels** déjà existants pour enrichir leurs fonctionnalités, par exemple :

- l'aide à la rédaction dans les logiciels de traitement de texte ou de messagerie ;
- la prédiction du risque de désabonnement dans les CRM (outil de gestion de la relation client) ;
- la détection d'erreurs dans les logiciels de comptabilité ;
- la suppression de certains éléments dans une image ou photographie dans les logiciels de traitement d'images.

2. L'usage de l'IA est-il réglementé ?

La mise en place d'un système d'intelligence artificielle doit notamment respecter les réglementations relatives à l'IA et à la protection des données personnelles mais aussi le droit du travail, dès lors qu'elle s'inscrit dans un cadre professionnel.

— Les niveaux de risques

La réglementation des IA en France et dans l'Union européenne repose principalement sur le **Règlement européen sur l'Intelligence Artificielle (RIA ou AI Act)⁸**.

(5) CNIL, *ibid.*

(6) "L'intelligence artificielle dite « générative » désigne les systèmes capables de créer des contenus (texte, code informatique, images, musique, audio, vidéos, etc.). Lorsqu'ils permettent de réaliser un large éventail de tâches, ces systèmes peuvent être qualifiés de systèmes d'intelligence artificielle à usage général. C'est par exemple le cas des systèmes intégrant des grands modèles de langage (en anglais large language models ou LLM)." CNIL, [Comment déployer une IA générative ? La CNIL apporte de premières précisions](#), 18 juillet 2024

(7) « Un *prompt* est une instruction, rédigée en langage naturel par un humain dans une interface homme machine (IHM), transmise à une IA générative pour interagir avec elle, afin d'obtenir une réponse. En fonction du type d'IA générative utilisée, cette réponse peut revêtir différentes formes : textes, codes informatiques, images, sons ou vidéos. », Délégation régionale académique au numérique éducatif, [IA générative : l'art du prompt](#), 4 mars 2024

(8) [Règlement \(UE\) 2024/1689](#) du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle



Pour aller plus loin

Article sur l'impact de l'AI Act pour le secteur des associations et fondations [«OSBL et intelligence artificielle : quelles réglementations et bonnes pratiques mettre en œuvre ?»](#), France générosités, 23 juillet 2024

Ce règlement encadre le développement, la mise sur le marché et l'utilisation des SIA susceptibles de présenter des risques pour la santé, la sécurité ou les droits fondamentaux. Il s'applique à toute organisation, que son objet soit lucratif ou non lucratif, déployant des SIA dans l'UE.

Concrètement, le RIA s'intéresse à l'utilisation et aux algorithmes d'utilisation des données. Il propose une approche fondée sur les risques en classant les SIA en quatre niveaux⁹.

Risque acceptable

IA interdite car contraire aux valeurs de l'Union européenne et aux droits fondamentaux¹⁰. Exemple : notation sociale, l'exploitation de la vulnérabilité des personnes, l'utilisation par les services répressifs de l'identification biométrique à distance en temps réel dans des espaces accessibles au public, etc.

Haut risque

IA susceptible de porter atteinte à la sécurité des personnes ou à leurs droits fondamentaux. En conséquence, leur développement et utilisation doivent être soumis à des exigences renforcées (évaluations de conformité, documentation technique, mécanismes de gestion des risques, étude d'impact). Pour le respect du RIA, certains traitements des données, classés à « haut risque », nécessitent une analyse d'impact (PIA/DPIA). C'est par exemple le cas

pour l'utilisation de certaines données en assurance.

Exemple : systèmes biométriques, systèmes utilisés dans le recrutement, ou pour le traitement de données sensibles (dont les données de santé).

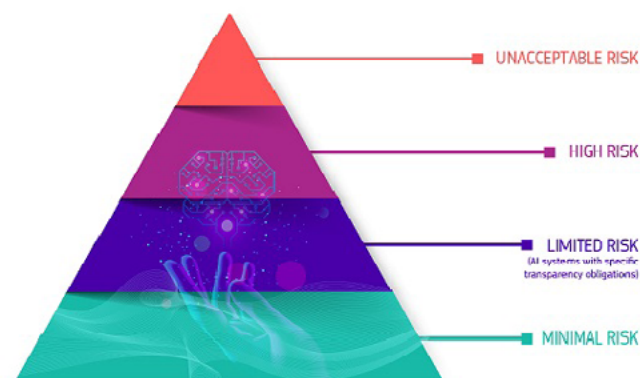
Risque spécifique en matière de transparence

Le RIA soumet des systèmes d'intelligence artificielle à des obligations de transparence spécifiques, notamment en cas de risque manifeste de manipulation.

Exemple : recours à des chatbots ou à la génération de contenu artificiel.

Risque minimal

Pour tous les autres SIA, le RIA ne prévoit pas d'obligation spécifique. Il s'agit de la très grande majorité des SIA actuellement utilisés dans l'UE ou susceptibles de l'être selon la Commission européenne.



Source : Commission européenne, [Législation sur l'IA](#)

(9) Commission européenne, [AI Act, A Risk-based Approach](#)

(10) « Le respect des droits fondamentaux est une exigence essentielle [du RIA] se manifestant de plusieurs manières : sans exhaustivité, il s'agit d'abord du respect de la dignité humaine et du droit à la vie privée, ensuite de la lutte contre les discriminations » JurisClasseur Communication, Fasc. 988 : Droit de l'intelligence artificielle (droit international et droit européen), Arnaud Latil, Maître de conférences HDR, Sorbonne Université, Chercheur au CERDI (Université de Saclay), 24 juillet 2024

— Les 7 grands principes éthiques

En complément de cette approche par les risques, le RIA définit sept grands principes éthiques devant être respectés par les systèmes d'intelligence artificielle.

1 Facteur humain et contrôle humain : Des mécanismes de surveillance appropriés doivent être mis en place, permettant une intervention humaine à différentes étapes de la modélisation et du déploiement des SIA (Cons. 66 & 73 - Articles 13 & 14 RIA).

2 Robustesse technique et sécurité : La résilience et la sécurité des SIA doivent être assurées. Leur sûreté, leur précision, leur fiabilité et leur reproductibilité doivent être garanties, et un plan de repli doit être prévu en cas de problème (Cons. 66 & 74 à 78 – Article 15 RIA).

3 Respect de la vie privée et gouvernance des données : Des mécanismes adéquats de gouvernance des données doivent être instaurés, en tenant compte de leur qualité et de leur intégrité, et en garantissant un accès légitime aux données (Cons. 66 à 70 - Article 10 RIA).

4 Transparence : Les SIA et leurs décisions doivent être expliqués de manière adaptée aux parties prenantes concernées. Les utilisateurs doivent être informés de leur interaction avec un SIA, ainsi que des capacités et des limites de celui-ci (Cons. 66 & 72 - Article 13 RIA).

5 Diversité, non-discrimination et équité : La diversité des utilisateurs et des données d'entraînement doit être favorisée, et les parties prenantes concernées doivent être associées tout au long du cycle de vie des SIA (Cons. 27 – Article 10 RIA).

6 Bien-être social et environnemental : L'impact des SIA sur l'environnement et la société doit être soigneusement évalué, en prenant en compte les autres êtres vivants et les conséquences sociales (Cons. 1 - Article 95 RIA).

7 Responsabilisation : L'auditabilité des algorithmes, des données et des processus de conception doit être assurée, notamment dans les applications critiques. Un recours adéquat et accessible doit être garanti pour toutes les parties concernées (Article 19 RIA).

L'utilisation d'un système d'intelligence artificielle est par ailleurs étroitement liée à la protection des données personnelles dès lors qu'un outil d'IA collecte, traite et stocke des données permettant d'identifier de manière directe ou indirecte des personnes physiques (adhérents, bénéficiaires, salariés, etc.).



Pour aller plus loin

[Mémento RGPD](#), France générosités, septembre 2020

A ce titre, les organismes sans but lucratif doivent respecter les principes du Règlement Général sur la Protection des Données (RGPD) et de la Loi informatique et libertés⁽¹⁾ lorsqu'ils recourent à un SIA susceptibles de traiter des données à caractère personnel :

- **légalité du traitement** : identification de la base légale du traitement (consentement, contrat, intérêt légitime, obligation légale, etc.) ;
- **respect des principes fondamentaux du RGPD** : minimisation, information des personnes concernées, limitation des durées de conservation, etc. ;

(1) [Règlement \(UE\) 2016/679](#) du Parlement européen et du Conseil du 30 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ; [Loi n° 78-17 du 6 janvier 1978](#) relative à l'informatique, aux fichiers et aux libertés

- **exercice des droits** : les personnes concernées doivent être en mesure d'exercer librement et facilement leurs droits (accès, rectification, effacement, opposition) ;
- **analyse d'impact (PIA/DPIA)** : si cela est nécessaire, la réalisation d'une analyse d'impact doit être réalisée (obligatoire si le traitement est "à haut risque").

Bonne pratique

Le RGPD et le RIA s'appliquent en même temps, nécessitant une cartographie exhaustive des outils d'IA et de leur usage des données personnelles.

— Les obligations vis-à-vis du droit du travail

Enfin, l'implémentation d'un système d'intelligence artificielle au sein d'un OSBL doit être **respectueuse du droit du travail applicable**. En effet, même en l'absence de disposition spécifique à l'intelligence artificielle, la mise en place de toute nouvelle technologie innovante impose le respect d'obligations, telles que :

Consultation et information du CSE

Le Comité social et économique (CSE) doit être consulté et informé sur les questions intéressant l'organisation, la gestion et la marche générale de l'entreprise, notamment sur **l'introduction de nouvelles technologies** (C. trav. art. L.2312-8, II, 4°). Ces informations et consultations doivent être réalisées dès la phase de projet. Ce dernier ne pourra être déployé qu'une fois que le CSE a rendu son avis sur les outils en question. Une jurisprudence a confirmé ce principe s'agissant d'un projet de déploiement de **nouvelles applications informatiques mettant en œuvre des procédés d'intelligence artificielle**¹² : la phase pilote a été suspendue jusqu'à la clôture de la consultation du CSE.

À noter

La notion de nouvelles technologies doit être appréciée « *par référence à l'entreprise et non de manière générale* » (CA Colmar, 16 janv. 1985). Le CSE est en droit de recourir à un expert habilité lorsqu'il est saisi d'un projet d'introduction de nouvelles technologies (C. trav., art. L. 2315-94, 2°).

Évaluation des risques professionnels

L'employeur doit intégrer tout nouveau risque lié à l'IA dans le Document Unique d'Évaluation des Risques Professionnels (DUERP). L'article L.4121-1 du Code du travail impose en effet d'identifier et de prévenir les risques pouvant affecter la santé et la sécurité des salariés – ce qui inclut désormais les conséquences des systèmes automatisés.

Gestion prévisionnelle des emplois et compétences (GEPP)

Dans les entreprises de 300 salariés et plus, une négociation obligatoire doit porter sur l'évolution des emplois et compétences (C. trav., art. L.2242-20). L'arrivée de l'IA modifiant souvent les tâches et compétences requises, cette négociation est renforcée pour anticiper les mutations professionnelles.

Information et formation des salariés

L'employeur a l'obligation d'informer et de former son personnel sur les changements liés au déploiement de l'IA. Cela inclut notamment l'explication des algorithmes utilisés (transparence, explicabilité) et la prévention des usages biaisés.

(12) TJ Nanterre, 14 févr. 2025, n° 24/01457 : JurisData n° 2025-001783

Adaptation du contrat de travail

Si l'IA modifie les conditions de travail (horaires, lieu, nature des tâches), il est nécessaire de consulter le CSE et d'obtenir l'accord des salariés concernés (modification du contrat). Les dispositions générales du Code du travail sur les changements technologiques s'appliquent.

3. Quelles opportunités pour quels usages ?

L'IA est un **outil d'assistance**. Présentée comme une technologie **libératrice des tâches à faible valeur ajoutée**, elle offrirait à ses utilisateurs un **gain général de productivité**. Les collaborateurs des OSBL pourraient ainsi consacrer davantage de temps à des tâches de réflexion et d'analyse et, d'une manière plus générale, à la réalisation de la mission sociale de l'organisation.

Les opportunités pour les OSBL sont multiples et l'IA peut s'inscrire dans le quotidien professionnel de l'ensemble de leurs salariés et bénévoles.

L'IA peut assister les collaborateurs dans la réalisation de missions génériques mais aussi dans des activités propres au secteur de la générosité.

— Exemples d'usages génériques de l'IA (liste non exhaustive)

La revue documentaire

- Analyser un corpus documentaire
- Synthétiser des documents
- Identifier la bibliographie adaptée
- Traduire des documents dans plusieurs langues
- Consolider en temps réel les évolutions de l'actualité via diverses sources

L'analyse, le nettoyage et la structuration de données

- Analyser de grands volumes de données

- Identifier des écarts, proposer des recommandations pour les corriger
- Structurer un ensemble de données brutes afin de le rendre exploitable
- Fiabiliser un jeu de données et les résultats en découlant, en évitant les erreurs dues à un traitement manuel
- Automatiser les tâches de reporting

La gestion de projet

- Modéliser des projets
- Identifier les moyens et ressources nécessaires
- Identifier les enjeux
- Définir le rythme des chantiers par rapport aux objectifs

Un support de réflexion dans la constitution de dossiers

- Réaliser un état des lieux interne, un benchmark externe et un état du marché
- Décrypter le contexte juridique et l'état de l'art
- Éclairer la prise de décision et favoriser l'initiative dans un périmètre observé plus finement et dans toutes ses composantes

— Exemples d'usages spécifiques aux OSBL faisant appel à la générosité (liste non exhaustive)

La gestion de la relation donateurs

- Mettre en place un chatbot sur le site d'une association pour répondre aux demandes simples des donateurs et remonter les demandes plus complexes qui nécessitent un traitement par un humain
- Aider les équipes à formuler et reformuler des réponses à des demandes de donateurs

La communication et le marketing

- Identifier les donateurs potentiels dans une base de données pour mieux les activer
- Analyser les évolutions des tendances et des pratiques afin d'adapter les leviers de communication

L'optimisation de l'impact auprès des bénéficiaires

- Traduire à l'écrit ou à l'oral (en passant par de la transcription) si la langue parlée par les bénéficiaires est différente de celles employées par les équipes afin de mieux comprendre leurs besoins et d'y répondre plus efficacement
- Analyser les pratiques des autres structures associatives, les attentes et besoins des bénéficiaires afin d'ajuster les actions à entreprendre
- Aider à l'interprétation des données des bénéficiaires afin d'orienter certaines actions, aide au diagnostic pour les associations médicales, etc.

La combinaison de ces usages peut constituer **un apport de technicité important pour les structures associatives qui disposent de ressources humaines et financières limitées.**

4. Comment sélectionner des outils d'intelligence artificielle conformes ?

Le choix éclairé des outils d'intelligence artificielle est d'autant plus crucial pour les OSBL, au regard des enjeux qui leurs sont propres (confidentialité, éthique, transparence, efficacité, etc.). Pour garantir une sélection et une mise en place responsable des outils, une méthode structurée peut être adoptée.

— Quel outil pour quel besoin : identification des besoins prioritaires des collaborateurs

Afin d'identifier les cas d'usage où l'IA apporte une réelle valeur ajoutée, il est essentiel de **cartographier les besoins concrets** des équipes opérationnelles et les attentes de la gouvernance.

Pour ce faire, la direction peut mener des entretiens ou sondages qui lui permettront de recenser les besoins récurrents des différents services (juridique, communication, gestion de projets, analyse de données, etc.) (cf. page 12).

Que souhaitent-ils accomplir précisément avec l'IA ? Quels usages et quels avantages concrets sont recherchés ? Quels outils sont susceptibles de répondre à ces besoins ? L'IA est-elle indispensable pour répondre à ces besoins ou un autre outil spécialisé peut-il les combler ? Comment la gouvernance compte-t-elle mettre en œuvre ces outils au quotidien ?

Bonne pratique

Au-delà des besoins, les usages actuels des collaborateurs doivent être recensés. En effet, les salariés et bénévoles ont pu s'emparer des outils d'IA en dehors de tout cadre managérial.

Il est également important de prendre conscience de l'omniprésence de l'IA dans les outils et technologies du quotidien. Que ce soit dans les logiciels de gestion, les plateformes de communication ou les outils d'analyse, l'IA est déjà intégrée, souvent de manière invisible.

Anticiper ses usages, c'est donc aussi cartographier les pratiques existantes au sein de ses différents services. Ces usages incontrôlés ou intégrés de l'IA doivent être répertoriés et analysés (cf. page 7 - Qu'est-ce que l'IA ?).

Une fois cette cartographie réalisée, la gouvernance peut s'interroger de manière plus précise sur sa vision stratégique de l'usage de l'IA.

— L'IA est-elle la seule solution pour répondre aux besoins identifiés ?

Avant de s'engager, l'OSBL doit explorer d'autres alternatives, qu'elles soient technologiques (outils existants non basés sur l'IA), organisationnelles (réorganisation des processus) ou humaines (renforcement des compétences internes).

Il est recommandé de réaliser des tests comparatifs entre différents outils (avec ou sans IA) pour évaluer objectivement leur efficacité, leur coût et leur adéquation avec les contraintes de l'association.

Certains outils généralistes (comme les LLM¹³ grand public) peuvent ne pas répondre à des besoins spécifiques (ex. : traitement de données sensibles, analyse sectorielle). Dans cette hypothèse, des solutions dédiées sont à explorer (ex. : outils d'analyse de données anonymisées, plateformes sécurisées pour les OSBL).

D'une manière générale, les outils à privilégier pour couvrir les besoins identifiés sont ceux qui y répondent de manière simple et efficace, sans surcharge fonctionnelle inutile. Les outils répondant à cette définition doivent ensuite être analysés pour s'assurer qu'ils respectent un minimum d'exigences en termes de conformité et de sécurité ainsi que les politiques et procédures internes (cf. page 26 - Comment construire un cadre responsable et éthique de l'usage de l'IA ?).

— Analyse du périmètre et de la provenance des données

La qualité et la sécurité des résultats dépendent directement des données utilisées par l'outil d'IA. Plusieurs questions sont à poser, telles que : quel périmètre est utilisé par l'outil pour générer des résultats ? Les données proviennent-elles de sources publiques, propriétaires ou internes à votre organisation ?

Certains outils s'appuient sur des bases de données génériques, tandis que d'autres permettent d'intégrer ses propres jeux de données (ex. : documents internes, bases de donateurs).

Bonne pratique

L'OSBL doit s'assurer que les sources utilisées par l'outil sont fiables, à jour et conformes à ses exigences. Il est recommandé de documenter le choix de l'outil en interne.

— La sécurité et la confidentialité des données sont-elles garanties ?

Les organisations d'intérêt général sont amenées à manipuler des données sensibles et des informations relatives à leurs parties prenantes (bénéficiaires, donateurs, partenaires, etc.). Il est donc crucial de s'assurer que l'outil sélectionné respecte des standards élevés de protection :

- Quelles sont les mesures et engagements du prestataire en matière de sécurité et de confidentialité ?
- Le chiffrement des données, des certifications

(13) Le modèle de langage est un modèle statistique de la distribution d'unités linguistiques (par exemple : lettres, phonèmes, mots) dans une langue naturelle. Un modèle de langage peut par exemple prédire le mot suivant dans une séquence de mots. On parle de modèles de langage de grande taille ou « Large Language Models » (LLM) en anglais pour les modèles possédant un grand nombre de paramètres (généralement de l'ordre du milliard de poids ou plus) comme GPT-3, BLOOM, Megatron NLG, Llama ou encore PaLM (CNIL, [Glossaire](#))

(ISO 27001) ou des audits de sécurité réguliers sont-ils réalisés ? Les conditions contractuelles proposées par le prestataire donneront des premiers éléments de réponse en la matière. Il revient à l'OSBL de vérifier les garanties offertes pour s'assurer du respect de standards minimums (ex. : clause de non-réutilisation des données).

- Les données transmises lors de l'utilisation de l'outil sont-elles utilisées pour entraîner le modèle ?
- L'historique des requêtes est-il conservé ?
- Si oui, pendant combien de temps ? Où sont stockées ces données ? Une suppression automatique ou un contrôle d'accès strict est-il possible ?
- Une licence entreprise est-elle requise pour assurer la confidentialité des données ?

 Certains outils exploitent les requêtes et données des utilisateurs pour entraîner et améliorer leurs algorithmes. Si des données sensibles ou confidentielles sont susceptibles d'être partagées par les collaborateurs de l'OSBL, des solutions qui n'utilisent pas ces inputs pour l'apprentissage sont à privilégier (opt-out ou modèles «privés»).

Bonne pratique

Les versions «grand public» des outils d'IA peuvent ne pas offrir le même niveau de protection que les versions professionnelles ou dédiées aux organisations. Il peut être nécessaire de souscrire une licence spécifique (ex. : «Enterprise», «NGO/ Non-profit») pour bénéficier de fonctionnalités sécurisées (ex. : espaces de travail isolés, administration centralisée).

— Estimation des coûts et de la viabilité économique

Les outils d'IA peuvent représenter un investissement significatif, surtout pour les structures à budget limité. Il est à ce titre recommandé :

- D'analyser les coûts associés à l'implémentation de l'outil sélectionné : certains outils fonctionnent par abonnements (coût mensuel/annuel), d'autres par crédits d'utilisation (pay-as-you-go).
- De comparer les tarifs en fonction du volume d'usage prévu et du budget de l'OSBL.
- De prendre en compte les coûts cachés (formation, intégration, maintenance).

— Mise en place de l'outil d'IA : tester avant de déployer

Aucun outil ne devrait être adopté sans une phase de test rigoureuse. Des tests en conditions réelles devraient ainsi être réalisés sur un périmètre restreint (ex. : un service, une campagne) avant tout déploiement à grande échelle d'un outil d'IA. A cette fin, un groupe pilote peut être constitué avec des collaborateurs volontaires pour évaluer les bénéfices de l'outil sur des cas concrets. Il est important de documenter les résultats de ces tests par le biais d'indicateurs :

- Pertinence des résultats : les réponses sont-elles utiles et fiables ?
- Facilité d'utilisation : l'interface est-elle intuitive ou nécessite-t-elle une formation dédiée ?
- Compatibilité de la solution avec les outils existants : intégration au CRM, à la suite bureautique, API, etc.
- Performances : temps de réponse, stabilité
- Risques imprévus

Ces tests permettront d'identifier d'éventuels points bloquants avant un déploiement à grande échelle.

Conclusion

En résumé, sélectionner un outil d'IA pour une organisation d'intérêt général exige une approche méthodique, centrée sur :

- ❶ Les besoins réels des équipes
- ❷ La sécurité et la confidentialité des données
- ❸ La transparence sur l'utilisation des données et l'historique
- ❹ La viabilité économique
- ❺ La validation par des tests concrets

Cette démarche garantit que les **outils choisis seront utiles, sûrs et alignés avec les valeurs et les contraintes de votre structure**. Il revient à chaque OSBL de personnaliser cette méthode avec tout autre critère qu'il estime nécessaire dans ce processus de sélection.

Étape 2



Cartographier les risques et évaluer la pertinence du recours à l'IA

Avant d'intégrer l'intelligence artificielle au sein de l'organisme sans but lucratif, il est essentiel d'engager une **réflexion collective et stratégique**, impliquant à la fois les équipes et la direction. Cette démarche permet de clarifier les enjeux, d'anticiper les risques et de définir un cadre d'usage adapté à ses missions et à ses valeurs.

La première étape consiste à **s'interroger sur la pertinence même de recourir à l'IA** : quels sont les cas d'usage concrets qui justifient son utilisation ? Quels bénéfices en attend-on ?

En partant des besoins et attentes des collaborateurs, il est possible de déterminer ce qui doit être autorisé, recommandé ou interdit, en fonction des spécificités des outils d'IA générative ou prédictive sélectionnés (cf. page 6 - "Quelles opportunités pour le secteur de la générosité ?").

La deuxième étape de la mise en place d'un outil d'IA au sein d'un OSBL consiste à mener une réflexion complémentaire autour de **trois questions centrales**.

1 Quels sont les risques intrinsèques liés à l'IA ?

Quelles externalités négatives sont susceptibles d'en découler (biais algorithmiques, protection des données, risques éthiques, dépendance aux outils, etc.) ?

2 Comment identifier les risques spécifiques à son association ou sa fondation ? Quels sont les vulnérabilités ou enjeux particuliers liés à la mission sociale, à la taille, aux publics cibles de l'OSBL ?

3 Comment évaluer le rapport bénéfice-risque de l'utilisation de l'IA ? Comment mettre en balance les avantages potentiels (gain de temps, amélioration des services) et les risques encourus (coûts cachés, impacts éthiques, complexité de mise en œuvre) ?

Cette approche méthodique permet d'aborder l'intégration de l'IA de manière réfléchie, responsable et alignée avec les valeurs et le contexte spécifique de son organisation.

1. Quels sont les risques intrinsèques liés à l'IA ?

Si l'IA offre des opportunités d'efficacité, elle comporte aussi des risques réels, notamment lorsque son usage se fait en dehors de tout cadre.

— Droits du travail, inégalités socio-économiques et transformation des métiers

« Selon le FMI, 62 % des emplois des économies avancées pourraient présenter un degré élevé d'exposition à l'IA. 27 % des emplois lui seraient fortement complémentaires et donc les plus à même de bénéficier de l'IA, tandis qu'elle pourrait se substituer à 33 % des emplois »¹⁴.

L'automatisation de certaines tâches, même partielle, peut conduire sur le long terme à une précarisation de certains métiers, à une intensification du travail ou à une perte d'autonomie pour les travailleurs. Par ailleurs, les inégalités socio-économiques peuvent être accentuées, certains métiers étant plus exposés au risque de substitution par des systèmes automatisés sans mécanismes sociaux de compensation ou de reconversion.



Pour aller plus loin

[Synthèse générale : Étude des impacts de l'IA sur le travail](#), LaborIA Explorer, 17 mai 2024

— Protection des données personnelles

L'intelligence artificielle fonctionne grâce à l'analyse de grandes quantités de données. Cela entraîne des risques de collecte excessive, de traitement sans consentement éclairé et, sur le long terme,

de fuites de données si les systèmes ne sont pas correctement sécurisés ou conformes aux réglementations applicables (RGPD et loi informatique et libertés). Ces risques sont particulièrement élevés lorsque des outils externes sont utilisés sans supervision, car des données sensibles peuvent être enregistrées ou réutilisées involontairement.

Pour aller plus loin



[Dossier CNIL «Intelligence artificielle \(IA\)»](#)

— Cybersécurité

L'utilisation de l'intelligence artificielle expose les organisations à des risques cyber accrus, souvent méconnus ou sous-estimés. Les outils d'IA, en manipulant des données sensibles (ex : donateurs, bénéficiaires, partenaires), peuvent devenir des portes d'entrée pour des cyberattaques : fuites de données via des modèles mal sécurisés, exploitation de vulnérabilités dans les algorithmes, ou encore détournement de systèmes automatisés pour diffuser des logiciels malveillants. Par ailleurs, les biais intégrés dans les modèles ou les erreurs de configuration (comme des accès non protégés) peuvent aggraver les failles, tandis que l'opacité de certains outils rend difficile la détection des intrusions. Pour les OSBL, souvent cibles privilégiées des cyberattaques, ces risques soulignent l'importance d'une vigilance renforcée.



Pour aller plus loin

[Les risques associés à l'usage de l'intelligence artificielle dans le monde professionnel](#), Direction générale de la sécurité intérieure (DGSi), décembre 2025

(14) TrésorEco n° 341, Les enjeux économiques de l'IA, avril 2024 et Conseil économique social et environnemental (CESE), [Étude Intelligence artificielle, emploi et travail](#), 14 janvier 2025.

— Impacts environnementaux

L'entraînement des systèmes d'intelligence artificielle mobilise des capacités de calcul et un volume de données conséquents. Cette activité qui s'exerce via le recours à des centres de données et des réseaux de serveurs engendre une consommation importante de ressources énergétiques (électricité, métaux rares et eau notamment). Cette consommation accrue d'eau et d'énergie contribue à l'empreinte carbone significative et par conséquent au coût environnemental des SIA.



Pour aller plus loin

[Quel est l'impact environnemental d'une IA générative ?](#), Délégation régionale académique au numérique éducatif, Région académique Ile-de-France, 7 novembre 2024

Un usage raisonné et l'attention portée à des pratiques plus durables (ex : entraîner ou déployer des modèles en tenant compte de leur efficacité énergétique, former les collaborateurs à la rédaction de prompts ou leur proposer des prompts prérédigés) sont essentiels pour réduire cet impact.

Le recours à des outils permettant de comparer les impacts environnementaux de l'IA est recommandé :

- [ComparIA du gouvernement](#)
- [EcoLogits de l'association GenAI Impact](#)

— Fiabilité de l'information et désinformation

Les outils d'intelligence artificielle peuvent produire des contenus erronés, ce qui peut propager de fausses informations si ces résultats ne sont pas vérifiés par une personne humaine. De plus, la simplicité de création de contenu automatisée peut être exploitée pour produire massivement de la désinformation.

Exemple : La BBC et l'Union européenne de radio-télévision (UER) ont réalisé une étude en 2025 avec 22 radiodiffuseurs de service public européens, dont Radio France, en soumettant 30 questions d'actualité à 4 assistants IA (ChatGPT, Copilot, Perplexity et Gemini). Ils ont ensuite analysé les réponses selon leur niveau d'exactitude, de contextualisation, la distinction entre les faits et les opinions ou encore selon la qualité des sources. 45 % de ces réponses présentaient au moins un problème significatif. Pour un cas sur cinq, il s'agissait d'informations obsolètes, de détails inventés ou de citations falsifiées. 31 % des réponses comportaient des attributions incorrectes ou trompeuses, souvent sans lien avec les sources originales¹⁵.



(15) BBC, [Representation of BBC News content in AI Assistants](#), 2025

— Propriété intellectuelle

L'IA utilise souvent des contenus préexistants pour apprendre et générer de nouveaux résultats. Cela pose des questions de propriété intellectuelle, notamment lorsque des œuvres ou des créations humaines sont utilisées sans attribution ni rémunération.



Pour aller plus loin

[Development of Generative Artificial Intelligence from a Copyright Perspective](#),
Office de l'Union européenne pour la propriété intellectuelle (EUIPO), mai 2025

— Adoption prématurée et dommages imprévus

L'introduction rapide ou mal encadrée d'outils d'IA peut mener à une dépendance technologique excessive ou à des erreurs de configuration qui perturbent les systèmes existants.

L'intégration avec les logiciels existants peut être complexe, et en l'absence de formation adéquate, les utilisateurs peuvent mal interpréter les résultats produits par ces systèmes, avec des conséquences opérationnelles ou juridiques.

2. Comment identifier les risques propres à son association ou sa fondation ?

L'intégration de l'IA dans les usages professionnels des organismes sans but lucratif exige une vigilance accrue. Au-delà des risques intrinsèques aux technologies d'IA, des risques supplémentaires s'appliquent au secteur de la générosité. Ces derniers sont étroitement liés aux missions sociales, aux valeurs et à l'éthique des associations et fondations, notions qui sont par définition propres à chacune d'entre elles.

A titre d'exemples, un OSBL œuvrant dans le médical ou le social devra prêter une attention particulière à la confidentialité des données (ex : dossiers patients, informations sociales sur le public accompagné), tandis qu'une structure axée sur le plaidoyer ou la communication devra anticiper les risques de désinformation ou de manipulation de contenus générés par l'IA.

Pour la gouvernance, l'enjeu est de définir ses enjeux stratégiques et d'exprimer des standards qui lui sont propres en matière d'IA, par le biais d'un guide ou d'une politique interne dédiée par exemple.

Cette étape est un préalable indispensable à l'identification des risques propres à l'OBSL.

C'est sur ce fondement que la gouvernance pourra ensuite s'interroger sur les éléments suivants :

- Quelles finalités ?
- Quels impacts ?
- Quel fonctionnement ?
- Quelles données ?
- Quelles garanties ?

— Quelles finalités ?

Déterminer de manière concrète, dès la genèse du projet, les finalités de l'usage projeté de l'IA en garantissant une utilisation responsable, transparente et alignée avec les principes réglementaires, éthiques et propres à son association ou sa fondation. A cette fin, des comités de pilotage de projets peuvent par exemple être mis en place.

— Quels impacts ?

A la lumière de la mission sociale de l'OSBL, les impacts liés à l'IA peuvent être évalués suivant une approche par les risques couvrant les dimensions économiques, juridiques, réputationnelles, organisationnelles, techniques et éthiques.

Risques juridiques et réglementaires

Il convient d'articuler de manière combinée, les dispositions du Règlement européen sur l'intelligence artificielle et du Règlement général sur la protection des données (Cf page 8) avec les réglementations propres au secteur dans lequel l'OSBL évolue. En effet, des législations sectorielles supplémentaires peuvent s'appliquer (recherche, santé, etc.).

Risques techniques et organisationnels

Il convient de réaliser une analyse des politiques de sécurité appliquées à l'outil d'IA (sa documentation complète), lesquelles permettront d'évaluer la protection des flux de données, la prévention des fuites et incidents sur les données, de déterminer la nécessité d'audits de sécurité, et le cas échéant, leurs périodicités.

Sur le plan organisationnel, il est important de s'interroger sur la conduite du changement à mener en interne. En cas de défaut de formation des équipes, l'outil d'IA peut-être mal utilisé ou inutilisé, ce qui contribuera à la réalisation des risques intrinsèques à l'IA (Cf. page 18).

Risques réputationnels et économiques

Il convient notamment :

- D'effectuer des due diligences relatives au prestataire avec lequel on envisage de contracter afin de s'assurer du respect des standards et éthique de l'OSBL (e-réputation, presse, etc.),
- D'évaluer les impacts économiques directs ou indirects des erreurs, décisions biaisées, ou encore des contenus non appropriés produits par les divers outils d'IA sur l'image de l'OSBL et sur la relation de confiance avec ses parties prenantes.

Risques éthiques

Il revient à l'OSBL de s'appuyer sur ses propres valeurs et principes qu'elle aura pu définir en interne, par exemple par le biais d'une charte éthique.

Enfin, il y a lieu de prendre en compte dans son évaluation les incidences environnementales résultant de l'utilisation des SIA.

— Quel fonctionnement (et quelle transparence du modèle) ?

La transparence et le fonctionnement d'un modèle d'IA soulèvent notamment les questions suivantes : Comment le modèle prend-t-il ses décisions, et sur quelles bases techniques repose-t-il (type, version, fournisseur, sources d'entraînement) ? Peut-il générer des biais, des stéréotypes ou encore des discriminations ? Une surveillance humaine est-elle mise en place pour surveiller ses actions ? Sommes-nous en mesure d'expliquer et justifier ses décisions ? Mais également, quelle sera la fréquence de ses mises à jour et existe-t-il un mécanisme de détection et d'évaluation d'éventuelles dérives ?

Chacune des réponses apportées à ces questions concourt à identifier les risques liés à la fiabilité et la conformité du système.

— Quelles données ?

Des risques supplémentaires peuvent exister en fonction des données qui seront utilisées et partagées avec les outils d'IA, ce qui **implique de clarifier leur nature et leur provenance**.

S'agit-il de données personnelles, sensibles ou confidentielles (rapports financiers, brevets, stratégies internes) ? Les données font-elles l'objet d'une anonymisation ou pseudonymisation ? Est-il possible de corriger ou supprimer les données partagées dans l'outil ? Les personnes concernées

À noter

D'autres questions peuvent émerger selon la typologie, la taille, les missions et les spécificités de son organisation, car chaque structure d'intérêt général présente des vulnérabilités et des enjeux distincts liés à l'usage de l'IA.

Par exemple, une association de petite taille, dotée de ressources limitées en matière de cybersécurité ou de conformité, devra s'interroger sur sa capacité à garantir la protection des données (ex : fichiers donateurs) ou à former ses équipes à des outils complexes, tout en évitant une dépendance technologique coûteuse. À l'inverse, une fondation ou un réseau associatif de grande envergure, manipulant des volumes importants de données sensibles, devra se pencher sur des risques plus systémiques : Comment sécuriser les échanges entre services ? Quels garde-fous mettre en place pour éviter les biais algorithmiques dans des décisions impactant des milliers de bénéficiaires ? Comment concilier innovation et respect des valeurs éthiques de l'organisation ?

sont-elles informées de l'utilisation de l'IA et de l'éventuel transfert hors Union Européenne de leurs données (lorsque l'outil utilisé est Américain par exemple) ? Qu'en est-il de l'usage des logs¹⁶, enregistrements vocaux et décisions automatisées au sens de l'article 22 du RGPD¹⁷ ?

— Quelles garanties ?

Se poser ces questions en amont de tout projet impliquant l'IA (Quelles finalités ? Quels impacts ? Quel fonctionnement ? Quelles données ?) **permet de cartographier ses risques spécifiques**.

Une fois l'ensemble des risques identifiés (intrinsèque à l'IA et propres à l'OSBL), des garanties doivent être associées à chacun d'entre eux par le biais d'un plan d'action à même de **transformer l'usage de l'IA en un levier sûr et maîtrisé, plutôt qu'en une source de vulnérabilités**.

Ce plan d'action peut inclure des mesures telles que la mise en œuvre de contrôles de conformité (RGPD, IA Act), audits réguliers, mécanismes d'explicabilité, clauses contractuelles renforcées, sécurisation des flux et des données, procédures de recours pour les personnes concernées, formations des acteurs, ainsi que des dispositifs de surveillance humaine et de détection des dérives. Ces garanties permettent de matérialiser la responsabilité et la transparence dans l'utilisation de l'IA.

(16) Le journal (en anglais log file ou plus simplement log), désigne alors le fichier contenant les enregistrements dans un fichier ou une base de données de tous les événements affectant un processus particulier informatique. [https://fr.wikipedia.org/wiki/Historique_\(informatique\)](https://fr.wikipedia.org/wiki/Historique_(informatique))

(17) <https://www.francegenosites.org/ressources/memento-rgpd/>

3. Comment évaluer le bénéfice-risque lié à l'utilisation de l'IA ?

Avant de se lancer dans l'adoption d'une solution d'IA, **l'association ou la fondation doit d'abord clarifier ses attentes et ses objectifs**. Elle doit par ailleurs s'interroger sur l'existence de **solutions alternatives à l'IA pour répondre à ces besoins** (Cf. Etape 1).

Si à l'issue de ces questionnements, l'IA est considérée comme la solution la plus adéquate pour répondre au besoin, il revient à l'OSBL d'évaluer le bénéfice/risques lié à ce choix.

— Une matrice bénéfice-risque...

Évaluer **le rapport bénéfice-risque de l'IA dans l'organisation** implique d'analyser l'équilibre entre les opportunités et les risques, qu'ils soient intrinsèques aux outils d'intelligence artificielle (Cf. page 18) ou propres à son organisation (Cf page 20).

Classer les opportunités et les risques selon leur impact (faible à élevé) et leur probabilité (peu probable à très probable) **permet de visualiser les scénarios acceptables et ceux à écarter**.

Exemple : Si un outil permet un gain de temps majeur (bénéfice) mais présente un risque élevé de fuite de données (risque), est-il envisageable de le déployer avec des garde-fous renforcés (ex. : anonymisation des données) ?

Une fois les bénéfices et les risques identifiés, il est nécessaire de les comparer les uns aux autres en fonction des priorités et contraintes de son organisation, mais aussi de vérifier ses résultats avec des tests pilotes avec les parties prenantes.

Bonne pratique

Une **mise à jour minutieuse et régulière de la cartographie des risques** est une démarche nécessaire avec, en particulier, une validation de la qualité des procédures de contrôle des risques liés à l'IA et du bon respect des principes de conformité. La matrice bénéfice-risque pourra être régulièrement revue sur cette base

— ... à coconstruire

Impliquer ses parties prenantes (collaborateurs, bénéficiaires et partenaires) dans la réflexion peut révéler des enjeux ignorés (ex. : réticence des équipes à utiliser l'outil, craintes des donateurs quant à la confidentialité).

Une analyse rigoureuse, combinant retours d'expérience, tests pilotes et consultation des parties prenantes **contribue à une prise de décision éclairée, justifiée et alignée avec les missions, les ressources et les valeurs de la structure**.

Une fois les enjeux identifiés, les risques évalués et les opportunités clarifiées, la question centrale devient : **comment traduire ces éléments en une gouvernance concrète, pérenne et responsable ?**

Cette démarche doit se concrétiser par des processus et des responsabilités claires pour garantir que l'IA soit déployée de manière éthique, sécurisée et maîtrisée dans la durée.

Étape 3



Comment mettre en place une gouvernance de l'IA ?

Les membres de la gouvernance des fondations et associations doivent pleinement prendre conscience de leurs responsabilités face aux enjeux numériques, singulièrement ceux relatifs à l'intelligence artificielle.

Il appartient à ces derniers d'être mobilisés et investis à chacune des grandes étapes de la mise en place d'un SIA :

- l'identification des cas d'usage concrets qui justifient son utilisation (cf. Etape 1),
- l'évaluation du bénéfice-risque de l'utilisation de l'IA au sein de l'OSBL (cf. Etape 2),
- jusqu'à la mise en place d'une gouvernance de l'IA (Etape 3, ici étudiée).

Tous les aspects de la gouvernance sont concernés : la raison d'être et la stratégie de l'organisation, le respect des principes éthiques, la gestion des opérations et des investissements ainsi que la maîtrise des risques.

La gouvernance de l'IA doit par ailleurs s'inscrire dans une démarche dynamique et proactive, où les politiques, les directives et les mécanismes de contrôle évoluent au rythme des avancées technologiques et des attentes des parties prenantes.

Ainsi, l'objectif de cette troisième étape est de donner les principales clés pour construire une gouvernance dédiée à l'IA via l'établissement de structures d'encadrement robustes contenant les politiques, les directives et les cadres d'exigences nécessaires. Il ne s'agit plus seulement de se demander si ou comment utiliser ces technologies, mais de définir une architecture claire de gestion, de supervision et de contrôle des SIA utilisés.

1. Comment définir et répartir les responsabilités ?

L'intégration de l'intelligence artificielle au sein d'un OSBL **implique une réflexion profonde sur la gouvernance**. Qui décide des usages de l'IA ? Qui en supervise la mise en œuvre ? Qui en assume les risques ? Sans une répartition claire des rôles et des responsabilités, les projets d'IA peuvent rapidement devenir sources de confusion, de désengagement, voire de risques juridiques ou éthiques.

Une **gouvernance solide repose sur l'implication de plusieurs niveaux de responsabilité**, chacun jouant un rôle complémentaire.

La structuration des responsabilités est à **personnaliser en fonction du contexte de chaque organisation**. Les repères suivants peuvent être pris en compte dans cette réflexion :

— La direction générale

Elle porte la vision stratégique et garantit que l'usage de l'IA s'aligne avec la mission, les valeurs et les objectifs de l'organisation. Les responsabilités sont les suivantes :

- valider les grands principes d'utilisation de l'IA (ex. : charte éthique, budget alloué) ;
- s'assurer que les projets d'IA respectent les enjeux juridiques (RGPD, RIA, etc.) et les engagements éthiques de la structure (ex : charte éthique) ;
- arbitrer en cas de conflits d'intérêts ou de désaccords sur les priorités.

— Un comité de pilotage dédié à l'IA

Il supervise la mise en œuvre des projets et en évalue l'impact, avec des représentants des services concernés (juridique, informatique, DSI, marketing, etc.), ainsi que des bénévoles ou bénéficiaires, si cela est pertinent.

Les responsabilités sont les suivantes :

- évaluer les opportunités et risques des projets d'IA (via des audits ou des tests pilotes, cf. page 13) ;
- prioriser les initiatives en fonction de leur alignement avec la stratégie globale ;
- rendre compte régulièrement à la direction et aux équipes.

— Les responsables métiers

Les responsables métiers ou de services (communication, programmes, finance, etc.) sont les relais opérationnels de l'IA dans leur domaine. Les responsabilités sont les suivantes :

- identifier les besoins concrets de leur service et proposer des cas d'usage pertinents ;
- former et accompagner leurs équipes à l'utilisation des outils ;
- remonter les alertes (ex. : dysfonctionnements, risques éthiques).

— Les équipes techniques

Les équipes techniques (informatique, DSI, data, etc.) garantissent la faisabilité technique et la sécurité des solutions. Les responsabilités sont les suivantes :

- choisir et configurer les outils adaptés aux besoins métiers ;
- sécuriser les données et veiller à la conformité réglementaire ;
- documenter les processus pour assurer la transparence.

— Les juristes et responsables conformité

Ils veillent au respect des cadres légaux (RGPD, RIA, droit du travail et toute autre réglementation sectorielle applicable). Les responsabilités sont les suivantes :

- valider les contrats avec les prestataires d'IA (clauses de confidentialité, propriété des données, sécurité, etc.) ;

- former les équipes aux obligations légales (ex : droits des personnes, analyse d'impact) ;
- auditer les outils pour détecter les risques juridiques.

— Les utilisateurs finaux

Les utilisateurs finaux (collaborateurs, bénévoles) utilisent l'IA de manière responsable et remontent les retours terrain. Les responsabilités sont les suivantes :

- suivre les bonnes pratiques définies par l'organisation (ex. : charte d'usage) et définir un cadre de sanction ;
- signaler les problèmes ou limites rencontrés.

Bonne pratique

L'ensemble des responsabilités peut être consigné dans un document de référence élaboré par la gouvernance pour éviter les flous et les chevauchements, tel qu'une charte d'usage de l'IA, des fiches de rôle et/ou encore un processus de décision.

Une gouvernance de l'IA efficiente et pertinente ne doit pas être figée. Il convient d'instaurer un suivi régulier, une évaluation des formalisations internes liées à l'IA (charte, fiches de rôle, processus, etc.) et un processus d'amélioration continue défini à l'avance (capitalisation des retours d'expérience, des tests, réévaluation des outils, formation continue, etc.).

2. Comment construire un cadre responsable et éthique de l'usage de l'IA ?

L'encadrement de l'utilisation de l'IA au sein d'un OSBL peut prendre différentes formes, telles qu'une charte éthique et/ou une politique d'usage.

Une **charte éthique** est un **document de principe qui formalise les valeurs, les engagements et les lignes directrices morales** d'une organisation concernant l'usage d'une technologie, ici l'IA. Elle vise à garantir que les pratiques sont alignées avec la mission sociale, les valeurs fondamentales et les attentes des parties prenantes.

Une **politique d'usage** est un **document opérationnel et contraignant** qui définit les règles pratiques, les procédures et les obligations liées à l'utilisation de l'IA au sein de l'organisation.

Bonne pratique

Une association ou une fondation peut commencer par construire sa charte éthique pour poser les bases, puis décliner ces principes en règles concrètes dans la politique d'usage. **Les deux documents doivent être cohérents et complémentaires** : la charte répond à la question : « Pourquoi et selon quelles valeurs utilisons-nous l'IA ? ». La politique répond à la question : « Comment utilisons-nous l'IA au quotidien, et quelles sont les règles ? »

Pour élaborer sa charte éthique et sa politique d'usage de l'IA, un certain nombre de grands principes devraient être respectés :

- Co-construire pour assurer l'efficacité et l'adhésion ;
- Définir les termes et créer un socle commun de compréhension ;
- Indiquer une méthode rigoureuse de sélection des outils d'IA ;
- Préciser les utilisateurs concernés par les principes édictés dans la charte (ex. : salariés, dirigeants, bénévoles) ;
- Clarifier les usages interdits et autorisés, avec un rappel des principes fondamentaux ;
- Lister les outils interdits et ceux autorisés, tout en prévoyant une granularité dans leur utilisation, par le biais d'une classification des informations par exemple,
- Présenter un inventaire des risques saillants ;
- Une charte éthique ou une politique d'usage efficace n'est pas figée et doit être revue régulièrement.

— La charte éthique

La **co-construction de ce document est essentielle pour en assurer l'adhésion et l'efficacité**, en impliquant l'ensemble des collaborateurs ou à défaut des représentants des différents services, afin de recueillir différentes perspectives. Cette approche collaborative permet de couvrir tous les angles, tout en renforçant la légitimité de la charte auprès des équipes. Les **organes représentatifs internes devraient aussi être mobilisés**, comme le Comité Social et Économique (CSE) - surtout si l'IA impacte les conditions de travail ou utilise les données à caractère personnel des salariés.

En intégrant ces acteurs dès le processus d'élaboration, l'organisation garantit le respect des droits des personnes concernées, prévient les éventuelles interrogations et résistances et, in fine, renforce la transparence et la confiance de chacun dans le projet.

Bonne pratique

Afin de poser un langage commun qui facilitera la compréhension des enjeux par tous, il est recommandé de définir en introduction de la charte **les termes clés utilisés dans le domaine de l'IA** (intelligence artificielle générative, machine learning, etc.).

Comme mentionné précédemment (Cf page 7), il est essentiel de souligner que les applications d'IA sont de plus en plus intégrées aux outils et logiciels professionnels existants pour enrichir leurs fonctionnalités. Cette réalité doit être prise en compte, car même si une association ou une fondation n'envisage pas d'utiliser directement l'IA, une **charte dédiée reste pertinente pour encadrer les usages indirects** et garantir une utilisation responsable de ces technologies.

— La politique d'usage

La **politique d'usage doit préciser une méthode rigoureuse de sélection des outils**, en s'appuyant par exemple sur les critères détaillés en annexe (sécurité, conformité, coût, éthique, etc.). Cette démarche permet d'éviter les choix hasardeux et de privilégier des solutions alignées avec les valeurs et répondant aux contraintes de l'organisation.

Ce document a notamment vocation à :

- préciser les **usages autorisés et ceux strictement interdits**, en définissant des limites nettes pour éviter toute ambiguïté ou dérive ;
- intégrer un **rappel des principes fondamentaux** régissant l'utilisation de l'IA afin d'ancrer ces valeurs dans les pratiques quotidiennes (respect de la vie privée, transparence, sobriété numérique, vérification systématique des résultats pour pallier les biais algorithmiques, etc.) ;
- **lister les outils approuvés** par l'organisation, en excluant explicitement ceux qui ne répondent pas aux critères de sécurité, d'éthique ou de conformité préalablement définis.

En complément, et selon la sensibilité des données manipulées, il peut être utile d'y inclure une **classification des informations** (par exemple, en catégories C1, C2, C3 selon leur niveau de confidentialité), afin de guider les collaborateurs sur les précautions à prendre en fonction des données traitées.

Enfin, pour sensibiliser les équipes aux enjeux liés à l'IA, le document peut présenter un **inventaire des risques saillants**, sans prétendre à l'exhaustivité, tels que les fuites de données, les biais discriminatoires, la dépendance technologique ou les non-conformités réglementaires. Cette approche permet aux utilisateurs de **comprendre les dangers** et d'adopter des comportements responsables, tout en offrant à l'organisation un cadre juridique solide pour agir en cas de manquement.

Pour être efficace dans le temps, les charte éthique et politique d'usage ne doivent pas être figées : elles s'enrichissent au gré des retours terrain et s'adaptent aux besoins émergents. A cette fin, **les modalités de révision régulières devraient être prévues dès la conception de ces documents**, avec des échéances claires et des mécanismes permettant aux collaborateurs de proposer des ajustements en fonction de l'évolution des usages, des technologies ou des réglementations.

3. Exemples de bonnes pratiques à inclure dans sa charte éthique ou sa politique d'usage dédiée à l'IA

Ce guide propose des **exemples de bonnes pratiques et de clauses à intégrer dans la charte éthique et/ou la politique d'usage d'IA** des OSBL. Prenant en compte les spécificités du secteur de la générosité, ces recommandations ont pour objectif de répondre à quatre grandes catégories de risques :

- Risques réglementaires (RGPD, RIA ACT, droits d'auteurs, etc.)
- Risques éthiques (confidentialité, transparence, désinformation, etc.)
- Risques professionnels (fiabilité, intelligibilité, sécurité, fuite des données, accès, etc.)
- Risques sociétaux (droits fondamentaux, recrutement, etc.)
- Risques environnementaux

— Risques réglementaires

D'une manière générale, la connaissance et le respect des réglementations ainsi que le respect des règles déontologiques doivent être garantis par les associations et fondations, en particulier dans l'utilisation des SIA. Cela implique notamment,

- **Le respect de la réglementation européenne sur l'IA**, et notamment des 7 principes éthiques énumérés par le RIA (cf. page 10).
- **La protection des données personnelles et des données sensibles** : des normes de sécurité rigoureuses doivent être respectées, conformément aux réglementations applicables en matière de protection des données. La vie privée des bienfaiteurs (donateurs, testateurs), des bénévoles, des salariés, des bénéficiaires et de toutes autres parties prenantes doit être préservée.

- **La protection des droits d'auteurs** lors de l'utilisation ou de la création de contenus générés par l'intelligence artificielle.

— Risques éthiques

Transparence à l'égard des utilisateurs finaux :

- **dans la communication** : les utilisateurs doivent notamment être clairement informés lorsqu'ils interagissent avec une intelligence artificielle ou lorsqu'une image ou un contenu lié à une campagne a été généré à l'aide de l'IA.
- **dans l'utilisation** : la transparence doit être démontrée dans le développement, le déploiement et l'utilisation des technologies d'IA. Des explications claires doivent être fournies sur les méthodologies, les résultats, les rapports, les mesures et les impacts potentiels de l'IA sur les utilisateurs finaux.

Définition des responsabilités : elles doivent être définies à chaque étape de la conception, du développement et du déploiement de l'IA, conformément aux cadres internes existants.

Éthique des données : des normes éthiques doivent être respectées en matière de collecte, d'analyse et d'utilisation des données (exactitude et pertinence des données, recueil du consentement).

Inclusivité et bienveillance : une démarche active contre les préjugés et les discriminations doit être menée tout au long du cycle de vie des SIA. Un cadre doit être développé pour surveiller et évaluer les SIA.

Bonne pratique

Une attention particulière doit être apportée aux outils reposant sur l'IA générative afin que ceux-ci soient utilisés de manière responsable. Aucun contenu entièrement rédigé par l'IA ne doit être publié sans contrôle ni retraitement humain : vérifications portant sur l'exactitude, la partialité, le ton et les éventuels plagiat.

— Risques professionnels

L'utilisation de l'IA, hors cadre défini par la politique interne, doit toujours être signalée au responsable de service, afin que les risques éventuels puissent être gérés de manière appropriée.

La sécurité de tout outil d'IA doit être évaluée avant son utilisation : les fonctionnalités de sécurité, les conditions d'utilisation et la politique de confidentialité de l'outil doivent être examinées. Tout outil d'IA utilisé doit respecter les normes de sécurité et de protection des données en vigueur. La réputation du développeur de l'outil, ainsi que celle des services tiers associés, doit également être vérifiée.

Seuls des outils d'IA réputés doivent être utilisés : une prudence particulière doit être exercée lors de l'utilisation d'outils développés par des personnes ou des entreprises dont la réputation n'est pas encore établie.

Aucune donnée confidentielle, exclusive ou protégée ne doit être téléchargée ou partagée dans un système d'intelligence artificielle sans information et accord préalable du service compétent. En toute hypothèse, de telles données ne peuvent être partagées qu'avec des solutions qui garantissent le cloisonnement des données et la non-réutilisation à des fins d'entraînement.

L'accès à des outils d'IA ne doit pas être accordé à des personnes extérieures à l'organisation sans l'accord préalable du service concerné ou du responsable référent. Les procédures requises pour respecter les exigences de conformité en matière de sécurité doivent être suivies, et aucun identifiant de connexion ou information sensible ne doit être partagé avec des tiers.

D'une manière générale, les bonnes pratiques de sécurité applicables à toutes les données de l'organisation doivent être pareillement respectées en matière d'IA par l'ensemble des parties prenantes (donateurs, collaborateurs, bénéficiaires, bénévoles, etc.). Cela inclut l'utilisation de mots de passe robustes, la mise à jour régulière des logiciels, ainsi que le respect des politiques de conservation et de suppression des données.

— Risques sociétaux

L'impact social positif de l'IA dans le domaine de la collecte de fonds et des missions sociales des organisations d'intérêt général doit être maximisé, tandis que tout préjudice potentiel doit être minimisé. Une attention particulière doit être portée aux besoins des bénéficiaires et des communautés concernées.

L'accès équitable à la technologie doit être garanti pour tous les membres de l'organisation et les parties prenantes.

Les préoccupations liées à la santé mentale des employés doivent être prises en considération et accompagnées de mesures adaptées, notamment en ce qui concerne :

- La crainte d'être remplacé par des machines (chômage technologique)
- Le sentiment de perte de pertinence professionnelle

La dignité humaine doit être respectée, en particulier dans le cadre de la surveillance liée à l'utilisation des technologies d'IA.

Lors des processus de recrutement, l'impact potentiel des biais présents dans les jeux de données des SIA doit être évalué et atténué.

La formation doit être assurée pour permettre aux employés de garder le contrôle sur les outils d'IA.

La sécurisation de l'emploi doit être garantie, afin que l'IA reste sous contrôle humain.

Une consultation en amont des salariés doit être organisée pour assurer la pertinence des systèmes d'intelligence artificielle et renforcer la confiance de tous.

— Risques environnementaux

La durabilité à long terme et l'impact environnemental des technologies d'IA doivent être pris en compte. A cette fin, des pratiques d'IA durables doivent être promues au sein de l'organisation d'intérêt général.

Sobriété de l'outil : des outils d'IA plus sobres doivent être privilégiés, notamment des modèles spécialisés, plus légers et moins énergivores. Les solutions open source doivent être favorisées pour encourager la réutilisation et limiter l'impact des phases d'entraînement, ainsi que les solutions françaises ou à *minima* européennes.

Sobriété dans l'usage : l'utilisation de l'IA doit être évaluée en amont pour déterminer si un autre outil ne serait pas plus adapté. Les utilisateurs doivent être formés à l'utilisation optimale des prompts (cf. page 6 - Etape 1).



Pour aller plus loin

[Comment bien prompter sur l'IA en 2026 pour éviter les risques et réduire son empreinte ?](#), France générosités, février 2026

L'impact environnemental des SIA doit être mesuré régulièrement à l'aide d'indicateurs tels que :

- Les ressources abiotiques,
- Le GWP (potentiel de réchauffement global et émissions de gaz à effet de serre),
- La consommation d'eau,
- La consommation d'énergie.

Pour les algorithmes, des outils comme Green Algorithms, Carbon Tracker, Code Carbon ou ML CO2 Impact peuvent être utilisés pour évaluer leur empreinte environnementale.

De nombreuses ressources et plusieurs référentiels d'organismes indépendants ou spécialisés sur l'IA existent afin de permettre de sélectionner les grands principes à inclure (voire exclure) au sein de sa politique interne de l'usage de l'intelligence artificielle.



Pour aller plus loin

- [Cadre de référence NIG \(numérique d'intérêt général\)](#) : en 21 critères caractérisés compatibles avec l'intérêt général
- [Framework toward Responsible and Beneficial AI](#) - Fundraising AI
- [Manifeste & cartographie](#) de Dial IA
- [RIA 31 : le référentiel IA - Éthique et Responsable](#) - INRC
- [Les ressources de Hub France](#)
- Le référentiel AFNOR - [31 fiches pratiques sur l'IA éthique et frugale](#)
- [Proposals for Global Governance on AI](#) - UN AI Advisory Body
- [IA for good](#)
- [Les ressources à venir du projet PANAME](#) de la CNIL, l'ANSSI, le PEReN et le projet IPoP du PEPR Cybersécurité

4. Comment intégrer et renouveler les procédures internes de l'OSBL pour un usage contrôlé de l'IA ?

— Procédures de contractualisation

Pour les associations et fondations, **l'utilisation de l'IA, qu'elle soit directe ou indirecte** (via des prestataires externes) soulève des enjeux juridiques, éthiques et opérationnels qu'il est **indispensable d'anticiper dans les contrats - que ce soit pour renégocier les accords existants ou pour élaborer de nouveaux contrats**. Une attention particulière doit être portée aux clauses liées à la protection des données, à la transparence des algorithmes et de l'usage de l'IA, à la responsabilité et à la conformité réglementaire.

Les OSBL qui travaillent déjà avec des prestataires (hébergeurs, éditeurs de logiciels, sous-traitants) utilisant ou intégrant des solutions d'IA doivent **auditer leurs contrats actuels pour s'assurer qu'ils couvrent les risques spécifiques** liés à ces technologies. A défaut, **un avenant devrait être signé avec le prestataire pour intégrer de nouvelles clauses**. Une renégociation peut également être organisée si les enjeux sont majeurs.

Lors de la sélection de nouveaux prestataires ou partenaires utilisant l'IA, les OSBL doivent intégrer dès la rédaction du contrat des garanties spécifiques pour se prémunir contre les risques.

En toute hypothèse, qu'il s'agisse de la révision d'un contrat existant ou d'une nouvelle contractualisation, une **approche rigoureuse et proactive** est à adopter par l'OSBL. Cela passe par :

- L'identification des risques (juridiques, éthiques, techniques)
- L'intégration de clauses protectrices (transparence, responsabilité, sobriété)
- La consultation des équipes internes (juridiques, métiers)
- Un suivi régulier des contrats pour les adapter aux évolutions technologiques et réglementaires

Les points clés suivants, spécifiques à l'usage de l'IA, devraient notamment être intégrés dans les contrats.

Une définition claire des usages autorisés de l'IA

Le contrat doit préciser quels outils d'IA seront utilisés, dans quel cadre (ex. : analyse de données, génération de contenus) et quelles données pourront être traitées. Toute utilisation en dehors de ce périmètre doit être interdite sans accord préalable.

La protection des données et la conformité réglementaire

Les contrats doivent explicitement préciser comment les données (notamment celles des donateurs, bénéficiaires ou salariés) sont collectées, traitées, stockées et supprimées par le prestataire. Il est crucial de vérifier que les clauses existantes sont conformes au RGPD et au RIA, et qu'elles imposent des mesures de sécurité renforcées (chiffrement, audits réguliers, limitation des accès). Si le prestataire utilise des outils d'IA générative ou prédictive, le contrat doit interdire toute réutilisation des données de l'OSBL pour entraîner ses modèles, sauf accord explicite.

La transparence

Les associations et fondations doivent exiger que le prestataire documente et explique le fonctionnement des algorithmes utilisés, notamment en ce qui concerne a minima :

- Les sources de données utilisées pour entraîner les modèles
- Les critères de décision des outils (ex : comment un algorithme classe-t-il les donateurs ?)
- Les limites et biais potentiels des SIA utilisés
- Une clause de transparence peut être ajoutée pour imposer au prestataire de fournir ces informations sur demande.
- La zone géographique dans laquelle les données vont être stockées et transitées. Vérifier si l'usage de certaines fonctionnalités d'IA entraîne un transfert en dehors de la zone géographique sélectionnée.

Une clause sur le droit d'audit peut être intégrée pour permettre à l'OSBL de vérifier régulièrement la conformité des traitements.

Les responsabilités et les recours

Les contrats doivent clarifier les obligations de chaque partie et prévoir des mécanismes de recours (indemnisation, résiliation) en cas d'erreur, de fuite de données ou de discrimination algorithmique. Par exemple, si un outil d'IA génère un contenu discriminatoire ou inexact, le prestataire doit s'engager à corriger rapidement le problème et à en assumer les conséquences. Une clause de limitation de responsabilité doit être évitée, ou du moins équilibrée pour protéger l'OSBL.

La propriété intellectuelle

Si l'IA est utilisée pour créer des contenus (textes, visuels, analyses), le contrat doit préciser qui détient les droits sur ces productions. Les OSBL devraient veiller à ce que les œuvres générées leur appartiennent pleinement, sans restriction d'usage.

Des garanties de sobriété et de durabilité

Les prestataires peuvent aussi s'engager, à la demande des organisations d'intérêt général, à utiliser des modèles d'IA sobres (peu gourmands en énergie) et à limiter leur empreinte carbone. Une clause peut imposer des audits environnementaux réguliers.

Une clause de révision périodique

Les technologies et réglementations évoluant rapidement, le contrat doit prévoir une révision sur une fréquence à définir (ex. annuelle) pour intégrer les nouvelles obligations légales ou les bonnes pratiques en matière d'IA demandées par l'OSBL qui contractualise.

Des critères supplémentaires

Des critères supplémentaires peuvent être imposés aux prestataires, tels que le respect de la Recommandation sur l'éthique de l'IA émise par l'UNESCO¹⁸, déjà adoptée par de nombreuses entreprises internationales.

En adoptant cette démarche, **les associations et fondations transforment la contractualisation en un levier de confiance et de sécurité**, et permettent d'éviter de nouvelles sources de vulnérabilités.

— Renouvellement des politiques internes

Pour construire des documents de référence pour la gouvernance et l'encadrement de l'usage de l'intelligence artificielle, l'organisation peut **mobiliser les outils et référentiels déjà en place comme leviers de réflexion et d'encadrement**. Ces dispositifs, issus du contrôle interne et/ou de la gouvernance, constituent une base solide qu'il convient de faire évoluer afin d'y intégrer l'IA dans un cadre cohérent et maîtrisé.

La charte informatique et la charte éthique existantes représentent des points d'appui précieux : elles traduisent déjà des engagements de transparence, de responsabilité et de respect des données. Leur analyse peut guider la formulation de principes spécifiques à l'IA, tels que la supervision humaine, la traçabilité des décisions automatisées ou la vigilance quant à l'accessibilité pour tous.

La cartographie des risques (si déjà existante) peut être examinée à travers le prisme de l'usage de l'IA : elle permet **d'identifier les zones de vulnérabilité** (biais algorithmiques, atteintes à la vie privée, etc.) et **d'anticiper les mesures de prévention à inscrire dans la charte**.

Cet exercice peut s'inspirer des méthodes déjà éprouvées dans la mise en conformité RGPD ou la sécurité des systèmes d'information, notamment à travers la logique de registre des traitements, qui aide à documenter les usages et à en justifier la légitimité.

(18) UNESCO, [Recommandation sur l'éthique de l'intelligence artificielle](#), 2022

5. Comment informer, sensibiliser et former les équipes opérationnelles à un usage responsable de l'IA ?

Former les collaborateurs des associations et fondations à l'intelligence artificielle est un levier essentiel pour en faire un outil au service de l'intérêt général, plutôt qu'une source de risques ou d'inefficacité.

Au-delà de la simple maîtrise technique, une formation permet de construire une **culture commune au sein de l'organisation, en démystifiant l'IA et en clarifiant ses enjeux, ses limites et ses opportunités**. Beaucoup de collaborateurs perçoivent encore ces technologies comme complexes, opaques, voire intimidantes ; les former, c'est leur donner les clés pour en comprendre les mécanismes, et ainsi désamorcer les craintes tout en évitant les usages naïfs ou inappropriés.

Sur le plan pratique, **une montée en compétences permet aux équipes d'optimiser leur utilisation de l'IA** : quels sont les outils pertinents à utiliser en fonction du besoin, quelles données utiliser ou ne pas utiliser, savoir formuler des prompts précis et efficaces, etc.

Bonne pratique

Une formation dédiée à la rédaction de prompt, permet d'obtenir des réponses adéquates plus rapidement (nombre de requêtes optimisé), de gagner en efficience (moins de temps perdu à corriger des résultats), mais aussi réduire l'empreinte environnementale des outils (moins de consommation énergétique grâce au nombre limité de requêtes). En ce sens, des « prompts

types » peuvent également être proposés aux utilisateurs (Voir aussi : [Comment bien prompter sur l'IA en 2026 pour éviter les risques et réduire son empreinte ?](#), France générosités, février 2026)

Enfin, la **formation joue un rôle clé dans la responsabilisation des utilisateurs**. En développant leur esprit critique, les collaborateurs apprennent à questionner les résultats générés par l'IA : ces données sont-elles fiables ? Biaisées ? Adaptées au contexte de l'OSBL ? **Cette vigilance collective est indispensable pour garantir que l'IA reste un levier d'action aligné avec les valeurs et la mission de l'organisation**, et non une boîte noire aux conséquences imprévisibles.

À noter

De nombreux formats d'animation au travail sont disponibles au sein de l'initiative [CaféIA](#) du Conseil National du Numérique (débat, post-its, jeux, écriture, projections, etc.)

Pour ancrer ces bonnes pratiques, il est recommandé d'**intégrer la formation au cœur de la politique interne d'usage de l'IA**, en y incluant des ressources pour l'autoformation (guides, tutoriels, webinaires) et en organisant des ateliers réguliers. Une organisation informée est une organisation protégée, et plus agile face aux défis de la transformation numérique.

Remerciements

Ce guide « Encadrer l'usage de l'IA au sein des associations et fondations » a été réalisé par France générosités en partenariat avec le Don en Confiance. Un grand nombre de personnes a été impliqué dans ce projet. Nous tenions à les remercier chaleureusement.

France générosités :

- Anouk Marchaland, juriste
- Corentin Hue, responsable digital et développement

Membres de France générosités :

- Sophie Mussard, AFM-Téléthon
- Virginie Poux, Médecins du Monde
- Redouane Bekrar, Amnesty International France
- Gaëlle Benoist, Médecins Sans Frontières

Don en Confiance :

- Anne-Lise Dudragne, responsable de projets

Bénévoles du Don en Confiance :

- Jacques Ethevenin
- Marie Menant
- Florence Picard

Liste des principales abréviations

CSE : Comité social et économique

DUERP : Document Unique d'Évaluation des Risques Professionnels

IA : intelligence artificielle

IAG : intelligence artificielle générative

OSBL : organisme sans but lucratif

RIA / AI Act : Règlement européen établissant des règles harmonisées

concernant l'intelligence artificielle

RGPD : Règlement Général sur la Protection des Données

SIA : système d'intelligence artificielle

Directrices de publication : Laurence Lepetit et Rachel Guez

Auteurs : Corentin Hue et Anouk Marchaland

Secrétaires de rédaction : Nadège Rodrigues et Sarah Bertail

Conception graphique : Claire Bourdon

Guide

Encadrer l'IA au sein des associations et fondations

Mars 2026

Réalisé par France générosités et le Don en Confiance, ce guide s'adresse aux associations et fondations qui souhaitent définir une politique interne d'usage de l'intelligence artificielle (IA) notamment générative (IAG).

Comment concilier usage de l'IA et respect des valeurs fondamentales ? Quels risques spécifiques les OSBL doivent-ils prévenir ? Quelle gouvernance de l'IA adopter ?... Conçu en trois parties indépendantes, ce guide adresse ces questions en donnant des repères basés sur les réglementations en vigueur et les bonnes pratiques du secteur de la générosité :

- Étape 1 : Quelles opportunités de l'IA pour le secteur de la générosité ?
- Étape 2 : Comment cartographier les risques et évaluer la pertinence du recours à l'IA ?
- Étape 3 : Comment mettre en place une gouvernance de l'IA ?



France générosités est le syndicat professionnel des organisations d'intérêt général faisant appel aux générosités. Il rassemble un réseau d'associations et de fondations philanthropiques œuvrant pour une société plus juste, inclusive et durable. www.francegenerosites.org



Depuis 1989, Don en Confiance renforce la confiance entre donateurs et organisations d'intérêt général en garantissant la transparence et la bonne utilisation des dons, grâce à un contrôle indépendant fondé sur une charte éthique exigeante. www.donenconfiance.org