



L'intelligence artificielle dans les associations et fondations : construire un usage responsable

(septembre 2026)

Que votre organisation découvre l'IA, engage une réflexion stratégique ou déploie déjà des outils, l'enjeu est de transformer une exposition passive à la technologie en usage maîtrisé.

L'intelligence artificielle (IA), et en particulier l'IA générative (IAG), s'installe rapidement dans les outils et pratiques des organismes sans but lucratif (OSBL). Cette adoption rapide soulève des questions techniques, juridiques et éthiques. Comment concilier innovation et respect des valeurs fondamentales ? Quels risques spécifiques prévenir ? Comment garantir un usage aligné avec la mission sociale et les engagements pris auprès des donateurs, bénéficiaires, bénévoles et partenaires ?

Trois grandes étapes structurent une démarche responsable d'intégration de l'IA au sein d'une association ou fondation*.

Comprendre l'IA et explorer ses opportunités

1 - Comprendre les mécanismes de l'IA

L'IA désigne un ensemble de technologies utilisant des données (textuelles, audio, vidéo) pour simuler l'intelligence humaine dans des tâches variées : apprentissage, raisonnement, résolution de problèmes, prise de décision. Elle se décline en plusieurs sous-domaines complémentaires qui peuvent être combinés (IA générative, machine learning, deep learning). Beaucoup d'outils professionnels intègrent déjà des fonctionnalités d'IA tels que l'aide à la rédaction dans les logiciels de messagerie, les prédictions dans les CRM, la détection d'erreurs en comptabilité ou le traitement d'images.

2 - Identifier des cas d'usage pertinents pour son organisation

Les opportunités pour les OSBL sont multiples : revue documentaire, analyse et structuration de données, gestion de projet, aide à la relation donateurs (chatbots, reformulation de réponses), communication et marketing, optimisation de l'impact auprès des bénéficiaires (traduction, aide à l'interprétation des données, aide au diagnostic). Cet apport de technicité peut particulièrement bénéficier aux structures aux ressources humaines et financières limitées. Avant tout déploiement, il est utile de cartographier les besoins concrets des équipes ainsi que les usages existants car les utilisations de l'IA existent probablement déjà en dehors de tout cadre.

3 - Connaître le cadre réglementaire applicable

Trois cadres se combinent et s'appliquent conjointement :

- Le **Règlement européen sur l'intelligence artificielle (RIA ou AI Act)**, qui classe les systèmes d'IA selon 4 niveaux de risque (inacceptable, haut, spécifique de transparence, minimal) et énonce 7 principes éthiques : facteur humain et contrôle humain, robustesse technique et sécurité, respect de la vie privée et gouvernance des données, transparence, diversité et non-discrimination, bien-être social et environnemental, responsabilisation.
- Le **RGPD** et la loi Informatique et Libertés, dès lors qu'un outil traite des données personnelles (identification de la base légale, minimisation, information des personnes, exercice des droits, analyse d'impact si nécessaire).

* France générosités et Don en Confiance les détaillent dans un [guide](#) co-publié en mars 2026.

- Le **droit du travail** : consultation du CSE en cas d'introduction de nouvelles technologies, mise à jour du [Document Unique d'Évaluation des Risques Professionnels](#), information et formation des salariés, éventuelle adaptation du contrat de travail.

4 - Sélectionner des outils conformes

Le choix d'un outil d'IA repose sur une méthode structurée : quels besoins réels des équipes ? L'IA est-elle la solution la plus adaptée ou une alternative existe-t-elle ? Quelle est la provenance des données utilisées par l'outil ? La sécurité et la confidentialité sont-elles garanties (chiffrement, cloisonnement des données, licence adaptée) ? Quels sont les coûts directs et cachés (abonnement, formation, intégration, maintenance) ? Un test sur un périmètre restreint, avec un groupe pilote et des indicateurs documentés, précède tout déploiement à grande échelle.

Évaluer les risques et la pertinence d'un déploiement

5 - Identifier les risques intrinsèques à l'IA

Ces risques concernent toute organisation qui déploie de l'IA :

- **Protection des données personnelles** : collecte excessive, traitement sans consentement éclairé, fuites, réutilisation involontaire pour l'entraînement des modèles.
- **Cybersécurité** : les outils d'IA peuvent devenir des portes d'entrée pour des cyberattaques, notamment via l'exploitation de vulnérabilités algorithmiques.
- **Impacts environnementaux** : consommation d'électricité, d'eau et de métaux rares liée à l'entraînement et au fonctionnement des modèles.
- **Fiabilité de l'information** : les IA génératives produisent parfois des contenus erronés ou biaisés**.
- **Propriété intellectuelle** : les modèles apprennent souvent à partir de contenus préexistants sans attribution ni rémunération de leurs auteurs.
- **Transformation des métiers** : automatisation de certaines tâches, précarisation possible, intensification du travail.

6 - Identifier les risques propres à son organisation

Au-delà de ces risques intrinsèques, chaque OSBL cartographie ses vulnérabilités spécifiques en fonction de sa mission, de sa taille et de ses publics cibles. Une structure médico-sociale portera une attention particulière à la confidentialité des dossiers ; une structure de plaidoyer anticipera les risques de désinformation ou de manipulation de contenus.

Cinq questions structurent cette réflexion :

- **Quelles finalités ?** Définir dès la genèse du projet à quoi servira concrètement l'IA.
- **Quels impacts ?** Évaluer les dimensions juridiques, techniques, organisationnelles, réputationnelles, économiques, éthiques et environnementales.
- **Quel fonctionnement ?** Comprendre les décisions du modèle, ses sources d'entraînement, ses biais possibles, la surveillance humaine mise en place.
- **Quelles données ?** Clarifier leur nature, leur provenance, leur sensibilité, les modalités d'information des personnes concernées.
- **Quelles garanties ?** Construire un plan d'action associant à chaque risque une mesure de mitigation.

7 - Évaluer le rapport bénéfice-risque

Une matrice bénéfice-risque, coconstruite avec les parties prenantes (collaborateurs, bénéficiaires, partenaires), permet de classer opportunités et risques selon leur impact et leur probabilité. Cette évaluation, régulièrement mise à jour, éclaire la décision de déployer ou de renoncer, et guide le choix des garde-fous à mettre en place (anonymisation des données, restriction d'usage, contrôle humain renforcé, sensibilisation des utilisateurs).

Mettre en place une gouvernance responsable

8 - Définir et répartir les responsabilités

Une gouvernance solide repose sur plusieurs niveaux d'implication complémentaires :

- **La direction générale** porte la vision stratégique et arbitre les priorités.
- **Un comité de pilotage dédié à l'IA** supervise la mise en œuvre des projets.
- **Les responsables métiers** relaient les usages dans leur service et remontent les alertes.
- **Les équipes techniques** garantissent la faisabilité et la sécurité des solutions.
- **Les juristes et responsables conformité** veillent au respect des cadres légaux.
- **Les utilisateurs finaux** appliquent les bonnes pratiques et signalent les difficultés rencontrées.

9 - Formaliser un cadre : charte éthique et politique d'usage

Deux documents complémentaires structurent l'encadrement :

- **La charte éthique** formalise les principes fondamentaux : respect de la vie privée, transparence dans la communication et l'utilisation, éthique des données, inclusivité et bienveillance, sobriété.
- **La politique d'usage** précise les usages autorisés et interdits, liste les outils approuvés, définit une classification des informations selon leur sensibilité, prévoit un cadre de sanction.

Ces documents sont coconstruits avec les représentants des équipes et les organes représentatifs internes (CSE), puis révisés régulièrement.

10 - Adapter les procédures internes

L'utilisation de l'IA, directe ou indirecte via des prestataires, impose d'auditer les contrats existants et d'intégrer des clauses spécifiques aux nouveaux contrats : périmètre d'usage autorisé, protection des données et conformité (RGPD, RIA), transparence sur les algorithmes et les zones de stockage, responsabilités et recours en cas d'erreur, propriété intellectuelle des contenus générés, sobriété énergétique, révision périodique.

11 - Sensibiliser et former les équipes

Une formation dédiée permet de démystifier l'IA, de développer l'esprit critique face aux résultats générés, d'optimiser l'usage (rédaction de prompts efficaces, réduction de l'empreinte environnementale). L'intégration de cette formation au cœur de la politique interne d'usage de l'IA contribue à faire d'une organisation informée une organisation plus agile face aux défis de la transformation numérique.

Deux principes traversent la démarche

La confiance des parties prenantes est le fil conducteur. Les OSBL agissent auprès de publics parfois vulnérables, mobilisent des données sensibles et reposent sur une relation de confiance avec leurs donateurs, bénévoles et partenaires. Chaque décision relative à l'IA gagne à être passée au crible de cette exigence.

La démarche s'inscrit dans la durée. Les technologies d'IA évoluent rapidement. Une veille régulière (technologique, réglementaire, sectorielle) et une révision périodique des cadres internes sont indispensables pour adapter les pratiques.

Don en Confiance pour le Crédit Mutuel

➤ Pour aller plus loin :

- [L'intelligence artificielle au service de la collecte de fonds : opportunités et précautions](#)
- [Ebook téléchargeable Numérique et IA : au service de l'impact associatif](#)