

GUIDE

IA générative en entreprise : éviter les fuites de données

Les risques de l'IA générative pour vos données, le cadre légal en clair (RGPD, règlement européen sur l'IA) et une feuille de route de gouvernance.

Sedona Radar — audit de sécurité externe automatisé

Sedona AI Lecture ~13 min Édition 2026 sedona-ai.com

Vos salariés utilisent déjà l'IA générative — la question n'est pas de savoir si, mais avec quelles garanties. Le vrai risque n'est pas la technologie : c'est l'usage non encadré, qui expose vos données confidentielles et vous met en tension avec le RGPD et le règlement européen sur l'IA. Ce guide montre comment capter les gains de l'IA générative tout en fermant les fuites, avec un cadre légal clair et une feuille de route de gouvernance actionnable pour une PME ou une ETI.

À retenir

- L'adoption est déjà massive et souvent invisible : le « shadow AI » (outils personnels utilisés au travail sans encadrement) est la norme, pas l'exception.
- Le risque principal est la fuite de données : tout ce qui est saisi dans un outil grand public peut être conservé, réutilisé pour l'entraînement, ou transféré hors UE.
- Le règlement européen sur l'IA impose depuis février 2025 une obligation de littératie : vos équipes doivent comprendre les outils qu'elles utilisent.
- Choisir une offre « entreprise » (pas de réentraînement sur vos données, hébergement UE, contrat de traitement) change radicalement le profil de risque.
- La gouvernance ne bride pas l'usage : elle le sécurise et le pérennise — cartographier, encadrer, outiller, former.

01 Le paradoxe de l'adoption

L'IA générative s'est diffusée plus vite que n'importe quelle technologie professionnelle récente — le plus souvent sans validation de la DSI. Résultat : des gains réels de productivité, mais aussi un angle mort de sécurité massif, le « shadow AI ».

75 %

Part des utilisateurs professionnels (« knowledge workers ») déclarant utiliser l'IA générative au travail.

Microsoft & LinkedIn, Work Trend Index 2024

78 %

Part des utilisateurs qui apportent leurs propres outils d'IA au travail (BYOAI), sans encadrement de l'entreprise.

Microsoft & LinkedIn, Work Trend Index 2024

27,4 %

Part des données d'entreprise envoyées vers des outils d'IA jugées sensibles en 2024 (contre 10,7 % un an plus tôt).

Cyberhaven, AI Adoption and Risk Report 2024

02 Les risques réels

Le danger n'est pas abstrait. Dès 2023, des ingénieurs de Samsung ont collé du code source confidentiel et le compte-rendu d'une réunion interne dans ChatGPT en l'espace de quelques semaines ; l'entreprise a fini par interdire l'usage des IA génératives grand public. Ce scénario — une donnée sensible saisie dans un outil qui la conserve et l'apprend — est le risque n°1 en entreprise.

- Fuite de données : secrets industriels, code source, données clients ou de santé collés dans un outil grand public, potentiellement conservés, réutilisés pour l'entraînement ou transférés hors UE.
- Hallucinations : des réponses fausses mais plausibles, dangereuses si elles ne sont pas vérifiées (juridique, chiffres, code).
- Injection d'invite (prompt injection) : des instructions malveillantes cachées dans un contenu externe détournent l'outil — classée risque n°1 par l'OWASP pour les applications à base de LLM.
- Dépendance et biais : décisions déléguées sans supervision humaine, reproduction de biais présents dans les données.

Le référentiel technique de référence

L'OWASP Top 10 for LLM Applications (2025) recense les risques spécifiques aux applications d'IA générative — en tête : l'injection d'invite (LLM01) et la divulgation d'informations sensibles (LLM02). Un bon point d'appui pour cadrer vos usages.

03 Le cadre légal en clair

Deux corpus s'appliquent cumulativement dès que des données personnelles entrent en jeu : le RGPD (déjà en vigueur) et le règlement européen sur l'IA (AI Act, règlement UE 2024/1689), dont les obligations entrent en application par étapes.

Échéance	Ce qui s'applique
1 août 2024	Entrée en vigueur du règlement sur l'IA.
2 février 2025	Interdiction des pratiques d'IA prohibées (art. 5) + obligation de littératie IA (art. 4) : le personnel doit disposer d'une compréhension suffisante des systèmes qu'il utilise.
2 août 2025	Obligations pour les modèles d'IA à usage général (GPAI, dont les grands modèles de langage) et gouvernance.
2 août 2026	Applicabilité générale du règlement ; les obligations pour les systèmes à haut risque s'échelonnent ensuite jusqu'en 2027-2028 selon les catégories.

Deux points concrets pour une PME

D'abord, l'obligation de littératie (art. 4) est déjà exigible : former vos équipes n'est pas optionnel. Ensuite, les sanctions du règlement sont lourdes (jusqu'à 35 M€ ou 7 % du chiffre d'affaires mondial pour les pratiques interdites). La CNIL a par ailleurs publié des fiches pratiques pour concilier IA et RGPD (finalisées en 2025).

04 7 règles pour un usage sûr

1 Classer avant de saisir

Définissez ce qui peut — et ne peut jamais — entrer dans un outil d'IA : jamais de secrets, code source, données personnelles de clients, données de santé ou financières dans un outil non maîtrisé.

2 Garder l'humain dans la boucle

Toute sortie d'IA est une proposition, pas une décision. Vérifiez systématiquement les faits, chiffres et sources avant usage.

3 Utiliser des comptes professionnels

Bannissez les comptes personnels : passez par des offres entreprise contractualisées, avec les bons paramètres de confidentialité.

4 Tracer les usages

Sachez quels outils sont utilisés, pour quoi, par qui — la traçabilité est la base de la maîtrise.

5 Se méfier des contenus externes

Un document ou un site peut contenir des instructions cachées (injection d'invite) : ne laissez pas l'IA agir sans contrôle sur des données non fiables.

6 Informer et fonder en droit

Associez le DPO : base légale, information des personnes, analyse d'impact (AIPD) si nécessaire, vérification des transferts hors UE.

7 Former les équipes

La littératie IA est une obligation (art. 4) et la meilleure défense : des salariés formés font moins d'erreurs que n'importe quel filtre technique.

05 Choisir un outil « entreprise » : la checklist

- ☐ Le fournisseur s'engage à ne pas réutiliser vos données (prompts) pour entraîner ses modèles.
- ☐ Les données sont hébergées et traitées dans l'Union européenne (ou avec un encadrement des transferts conforme au RGPD).
- ☐ Un contrat de traitement des données (DPA) est disponible et signé.
- ☐ La conservation des données est paramétrable (durée, désactivation de l'historique).
- ☐ L'accès est protégé par le MFA et une gestion des rôles ; les usages sont journalisés.
- ☐ Le fournisseur documente ses mesures de sécurité et sa conformité (RGPD, éventuellement certifications).

06 Feuille de route gouvernance

1 Cartographier

Recensez les usages réels de l'IA dans l'entreprise, y compris le shadow AI, sans esprit de sanction — pour révéler la réalité.

2 Désigner un référent IA

Une personne responsable de la doctrine IA, du choix des outils validés et du lien avec le DPO.

3 Publier une charte

Un document court et clair : outils autorisés, données interdites en entrée, règles d'usage, responsabilités (voir notre modèle de charte).

4 Outiller et former

Fournir les bons outils entreprise ET former les équipes (obligation de littératie) : c'est le couple qui élimine le shadow AI.

Interdire ne marche pas, encadrer oui

Bloquer purement et simplement l'IA pousse les usages dans l'ombre. La bonne approche : offrir un chemin sûr (outils validés + charte + formation) plus pratique que le contournement.

§ Sources

1. Règlement (UE) 2024/1689 sur l'intelligence artificielle (AI Act) — <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
2. Commission européenne — Cadre réglementaire de l'IA et calendrier — <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>
3. CNIL — Les fiches pratiques IA (conformité RGPD) — <https://www.cnil.fr/fr/les-fiches-pratiques-ia>
4. OWASP — Top 10 for LLM Applications 2025 — <https://genai.owasp.org/resource/owasp-top-10-for-llm-applications-2025/>
5. Microsoft & LinkedIn — 2024 Work Trend Index — <https://www.microsoft.com/en-us/worklab/work-trend-index/>
6. Cyberhaven — AI Adoption and Risk Report (2024) — <https://www.cyberhaven.com/blog/4-2-of-workers-have-pasted-company-data-into-chatgpt>
7. Forbes — Samsung bans ChatGPT after code leak (2023) — <https://www.forbes.com/sites/siladityaray/2023/05/02/samsung-bans-chatgpt-and-other-chatbots-for-employees-after-sensitive-code-leak/>
8. ENISA — Artificial Intelligence Cybersecurity Challenges — <https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges>

Commencez par voir ce que vous exposez

Une IA mal encadrée expose vos données de l'intérieur ; un domaine mal configuré les expose de l'extérieur. Sedona Radar analyse ce que votre domaine expose sur Internet et remet un rapport en français, avec un plan de correction. Lancez un scan gratuit.

Lancer mon scan gratuit

sedona-ai.com/scan-gratuit