

IA générative au travail : les règles d'usage

ChatGPT et consorts sont déjà utilisés dans vos équipes. Encadrer plutôt qu'interdire — sans fuiter vos données.

9 min de lecture · Niveau Essentiel · cyberionis.fr/ressources/ia-generative

Que vous l'ayez décidé ou non, vos collaborateurs utilisent probablement déjà des assistants IA pour rédiger, traduire ou résumer. Le risque n'est pas l'outil : c'est ce qu'on y colle. Un contrat client copié dans un chatbot grand public est une donnée qui sort de l'entreprise.

1. Les risques concrets

- Fuite de données : informations clients, contrats, code source ou données RH collés dans un outil qui peut les conserver, voire s'en servir pour s'entraîner
- Shadow AI : des comptes personnels gratuits utilisés pour le travail, hors de tout contrôle de l'entreprise
- Réponses erronées présentées avec assurance : chiffres inventés, références juridiques inexistantes
- Non-conformité RGPD si des données personnelles sont traitées sans base légale ni information des personnes

2. Poser un cadre simple

L'interdiction pure pousse à l'usage caché — sur téléphone personnel, sans aucun garde-fou. Mieux vaut un cadre clair tenant sur une page :

- Choisir un ou deux outils validés par l'entreprise, avec des comptes professionnels (les offres entreprise s'engagent contractuellement à ne pas entraîner leurs modèles sur vos données)
- Interdire d'y saisir : données clients nominatives, données de santé, secrets industriels, identifiants, données financières non publiques
- Exiger une relecture humaine de tout contenu produit avant envoi ou publication
- Désactiver l'historique/l'entraînement quand l'option existe

3. L'IA côté attaquants

L'IA générative profite aussi aux fraudeurs : emails de phishing sans fautes, faux sites crédibles en quelques minutes, et désormais deepfakes audio ou vidéo imitant la voix d'un dirigeant pour ordonner un virement. Raison de plus pour ancrer les procédures de vérification (rappel au numéro connu, double validation) qui ne reposent pas sur « je reconnais sa voix ».

4. Le RGPD s'applique aussi aux prompts

Saisir des données personnelles dans un outil d'IA est un traitement au sens du RGPD : il lui faut une base légale, une information des personnes et un sous-traitant encadré. Le règlement européen sur l'IA (AI Act) ajoute progressivement ses propres obligations, notamment la transparence sur les contenus générés.

- Pas de données clients nominatives dans un outil non couvert par un contrat de sous-traitance (DPA)
- Anonymiser avant de soumettre : « un client du secteur BTP » plutôt que le nom de l'entreprise et du contact
- Vérifier où l'outil héberge et conserve les conversations
- Mentionner l'usage d'outils d'IA dans le registre des traitements si des données personnelles y transitent

ATTENTION

Un texte généré par IA peut être faux avec aplomb : chiffres inventés, jurisprudences inexistantes, références plausibles mais fictives. Pour tout contenu engageant l'entreprise — devis, contrat, conseil client, communication — la relecture par un humain compétent n'est pas une option, c'est le garde-fou.

L'essentiel à retenir

- 01 Valider un ou deux outils IA avec des comptes professionnels
- 02 Lister noir sur blanc les données interdites de saisie
- 03 Anonymiser les cas clients avant de les soumettre
- 04 Imposer la relecture humaine avant toute diffusion
- 05 Sensibiliser aux deepfakes dans les procédures de paiement
- 06 Intégrer l'usage de l'IA à la charte informatique

Questions fréquentes

Interdire complètement l'IA ne serait-il pas plus simple ?

L'interdiction totale a un effet pervers documenté : l'usage continue en caché, sur téléphones et comptes personnels, sans aucun garde-fou — c'est le « shadow AI ». Un cadre clair avec des outils validés canalise l'usage là où vous pouvez le contrôler, et vos équipes gagnent réellement du temps sur les tâches d'écriture et de synthèse.

Les versions payantes protègent-elles vraiment mieux les données ?

Les offres entreprise s'engagent contractuellement : pas d'entraînement des modèles sur vos données, hébergement défini, contrat de sous-traitance RGPD, contrôles d'administration. Les versions gratuites grand public n'offrent aucune de ces garanties par défaut. La différence n'est pas le modèle d'IA, c'est le contrat.

Comment reconnaître un deepfake audio ou vidéo ?

De moins en moins à l'oreille ou à l'œil — la technologie progresse trop vite. La parade n'est pas la détection mais la procédure : aucune action sensible (virement, communication d'identifiants, changement de RIB) déclenchée sur la seule base d'un appel ou d'une visio, même avec la voix et le visage « du patron ». On raccroche et on rappelle au numéro connu.

Peut-on utiliser l'IA pour écrire du code ou configurer nos systèmes ?

Oui, avec les mêmes règles : jamais de secrets (mots de passe, clés d'API, configurations sensibles) dans les prompts, et une revue par quelqu'un qui comprend le code produit — l'IA reproduit aussi des schémas non sécurisés. Pour le code métier sensible, préférez les offres qui garantissent la non-réutilisation de vos données.

Pour aller plus loin

CNIL — recommandations sur l'IA — www.cnil.fr/fr/intelligence-artificielle

ANSSI — recommandations de sécurité pour l'IA générative — cyber.gouv.fr/publications/recommandations-de-securite-pour-un-systeme-dia-generative

Besoin d'aide pour le mettre en place ?

Audit, durcissement, accompagnement : Cyberionis sécurise les TPE, PME et collectivités, à Nancy, Lure et à distance.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr