

Charte de bonnes pratiques — Utiliser l'IA en toute sécurité

À destination des équipes de TPE et PME. Une page, à lire, appliquer et signer ensemble.

1. Objet et périmètre

Cette charte fixe les règles minimales à respecter par toute personne de l'entreprise utilisant un outil d'intelligence artificielle générative (ChatGPT, Claude, ou tout autre assistant IA) dans le cadre de son travail.

Objectif : réduire le risque de fuite de données sensibles à un niveau maîtrisé. Aucune solution n'offre un risque zéro — cette charte ne le promet pas non plus.

2. Les données à ne JAMAIS coller telles quelles dans une IA

- Données clients nominatives (noms, coordonnées, historiques d'achat)
- Données RH (salaires, évaluations, arrêts maladie, données disciplinaires)
- Données financières précises (comptes bancaires, chiffres non publics)
- Clauses contractuelles sensibles (prix négociés, conditions de confidentialité)
- Mots de passe, identifiants, clés d'accès — jamais, même anonymisés

3. Comment anonymiser en pratique : la règle des dix secondes

Avant de coller un texte dans une IA, prenez dix secondes pour :

- Remplacer les noms propres par des repères génériques (« Client A », « Salarié X »)
- Remplacer les montants précis par des ordres de grandeur
- Remplacer les dates exactes par des périodes approximatives

Si le texte ne peut pas être anonymisé sans perdre son sens, c'est probablement qu'il ne doit pas être collé du tout.

4. Réglages de confidentialité à activer

Le type de compte change tout. Un abonnement personnel payant (ChatGPT Plus, Claude Pro) ne protège pas vos données par défaut : elles peuvent servir à entraîner les modèles, sauf désactivation manuelle.

- Privilégier un compte professionnel validé par l'entreprise (Claude for Work, ChatGPT Business/Enterprise) plutôt qu'un compte personnel
- Sur un compte personnel, vérifier et désactiver le réglage d'entraînement dans les paramètres de confidentialité
- Ne jamais laisser de commentaire (pouce vers le haut/bas) sur une conversation contenant une donnée sensible : cela déclenche une conservation prolongée de toute la conversation, quel que soit le réglage d'entraînement

5. Règles d'équipe

- Un seul outil IA « autorisé » par l'entreprise pour les usages professionnels — pas de choix individuel non validé

- Toute nouvelle utilisation d'IA sur une donnée sensible est validée au préalable par le responsable désigné
- Cette charte est relue avec chaque nouvel arrivant avant sa prise de poste

6. Que faire en cas de doute ou d'incident

Si une donnée sensible a été collée par erreur dans une IA :

- Supprimer immédiatement la conversation
- Prévenir sans délai le responsable sécurité / conformité de l'entreprise — même sans certitude que ce soit grave

Un signalement maladroit vaut toujours mieux qu'un silence qui laisse le problème grandir.

7. Engagement de l'équipe

En signant ci-dessous, chaque membre de l'équipe atteste avoir lu cette charte et s'engage à en respecter les règles.

Nom	Signature	Date

Version 1.0 — Document créé le 8 juillet 2026. À redater à chaque révision.

Cette charte accompagne l'article « Comment utiliser l'IA en entreprise sans compromettre vos données sensibles ? » — Learning Lagoon.