Protéger ses données avec les outils d’IA : 5 bonnes pratiques simples

Synthèse générée par Mia, chatbot d’Annemasse Agglo

Protéger ses données avec les outils d’IA : 5 bonnes pratiques simples

L’IA est partout : chatbots, générateurs d’images, assistants vocaux, outils de traduction automatique… Ces services analysent ce que vous leur donnez. Voici comment les utiliser sans exposer vos données personnelles.

1. Ne jamais partager de données sensibles

À éviter absolument :

- Noms, adresses, numéros de téléphone, emails, dates de naissance.
- Données médicales, financières (RIB, numéros de carte bancaire) ou administratives (numéro de sécurité sociale).
- Photos ou documents personnels (scans de pièces d’identité, contrats, relevés bancaires).

À faire :

- **Anonymisez vos demandes** :
  - *"Je m’appelle Martin Dupont, j’ai 35 ans et je vis à Annemasse. Quels sont les risques pour ma santé ?"*
  - *"Quels sont les risques pour la santé d’une personne de 35 ans ?"*
- **Évitez les fichiers personnels** : ne téléchargez pas de PDF, images ou documents contenant des informations privées.

2. Utiliser des comptes dédiés et temporaires

Créez un email spécifique pour les outils d’IA (ex. : monia.ia@protonmail.com).

Ne liez pas vos comptes (Google, Facebook, Apple) à ces services.

Supprimez votre historique après chaque utilisation (hors projets) :

- Cherchez l’option *"Supprimer mes données"* ou *"Effacer l’historique"* dans les paramètres.

3. Désactiver la mémorisation et le partage des données

Désactivez l’apprentissage automatique (si possible) :

- Certains outils (comme ChatGPT) permettent de désactiver l’utilisation de vos conversations pour améliorer leurs modèles. Activez cette option dans les paramètres.
- Exemple de chemin possible : *Paramètres > Confidentialité > Désactiver "Améliorer le modèle avec mes conversations"*.

Refusez le partage de données avec des tiers :

- Dans les paramètres de l’outil, vérifiez que l’option *"Partager mes données avec des partenaires"* est désactivée.

Utilisez des outils en mode privé :

- Certains outils (comme DeepL) proposent un mode privé qui ne stocke pas vos requêtes. Activez-le systématiquement.

4. Privilégier les outils locaux ou open source

Les outils d'IA locaux (installés sur votre ordinateur) ou open source (transparents sur leur fonctionnement) limitent les risques de fuite de données, car vos informations ne quittent pas votre appareil.

Besoin	Outil classique	Alternative locale/open source	Pourquoi ?
Chatbot	ChatGPT, Bard	LocalAI, Ollama	Fonctionne sur votre ordinateur, pas de cloud.
Génération d'images	MidJourney, DALL·E	Stable Diffusion (local)	Pas d'envoi de vos images à des serveurs externes.
Traduction	Google Translate	LibreTranslate (auto-hébergé)	Respectueux de la vie privée.
Assistant vocal	Siri, Alexa	Mycroft (open source)	Pas de cloud, données locales.

5. Vérifier et supprimer ses données régulièrement

Demandez la suppression de vos données :

- Contactez le service via son formulaire RGPD (ex. : formulaire OpenAI).
- Modèle de demande :

Objet : Demande de suppression de mes données personnelles Madame, Monsieur, Conformément à l'article 17 du RGPD, je vous demande de supprimer l'intégralité des données personnelles que vous détenez me concernant, collectées via [nom du service]. Merci de me confirmer par retour la prise en compte de ma demande. Cordialement, [Votre nom]

Utilisez des outils pour vérifier les fuites :

- **Have I Been Pwned** : Vérifiez si votre email a fuité.
- **Firefox Monitor** : Recevez des alertes en cas de fuite de données.

Checklist rapide

- ☐ Je n'ai jamais partagé de données sensibles (nom, adresse, numéro de téléphone, etc.).
- ☐ J'ai anonymisé mes demandes (pas de détails personnels inutiles).
- ☐ J'utilise un email dédié pour les outils d'IA.
- ☐ J'ai désactivé l'historique et la mémorisation des conversations.
- ☐ J'ai désactivé le partage de données avec des tiers.
- ☐ J'utilise des outils locaux ou open source quand c'est possible.
- ☐ J'ai supprimé mes données après utilisation.