



CHECKLIST IMPRIMABLE

IA & données personnelles : le contrôle à faire avant chaque envoi

Avant de coller un prompt, d'importer un fichier ou d'activer un connecteur, passez cette checklist en revue. Elle aide à tirer parti de l'IA sans exposer inutilement votre vie privée, vos accès ou les informations de votre organisation.

Au sommaire

- 1 1. Identifier ce que contient votre demande
- 2 2. Écarter les contenus à ne pas transmettre
- 3 3. Réduire et anonymiser avant l'envoi
- 4 4. Vérifier l'outil et le compte
- 5 Repères rapides : partager ou reformuler ?
- 6 En cas d'envoi accidentel

1. Identifier ce que contient votre demande

- ☐ **Repérer les identifiants directs**
Nom, adresse e-mail, numéro de téléphone, identifiant de compte ou document d'identité.
- ☐ **Repérer les identifiants indirects**
Fonction, employeur, lieu précis, date, référence de dossier, historique ou contexte pouvant permettre un recoupement.
- ☐ **Vérifier si une personne peut être reconnue grâce à l'ensemble du contexte**
Remplacer un nom par une initiale ne suffit pas nécessairement à anonymiser un document.
- ☐ **Distinguer les données de l'utilisateur de celles de tiers**
Clients, salariés, patients, partenaires et autres personnes concernées demandent une attention particulière.

2. Écarter les contenus à ne pas transmettre

- ☐ **Ne jamais saisir de mot de passe, code à usage unique ou clé d'API**
- ☐ **Ne pas envoyer de dossier médical, donnée biométrique ou information concernant un mineur**
- ☐ **Écarter les relevés bancaires, justificatifs d'identité et informations financières sensibles**
- ☐ **Ne pas importer un document personnel complet ou une information de sécurité**
- ☐ **Mettre de côté les données confidentielles ou stratégiques de l'organisation**
Demander une validation interne si le contexte l'exige.

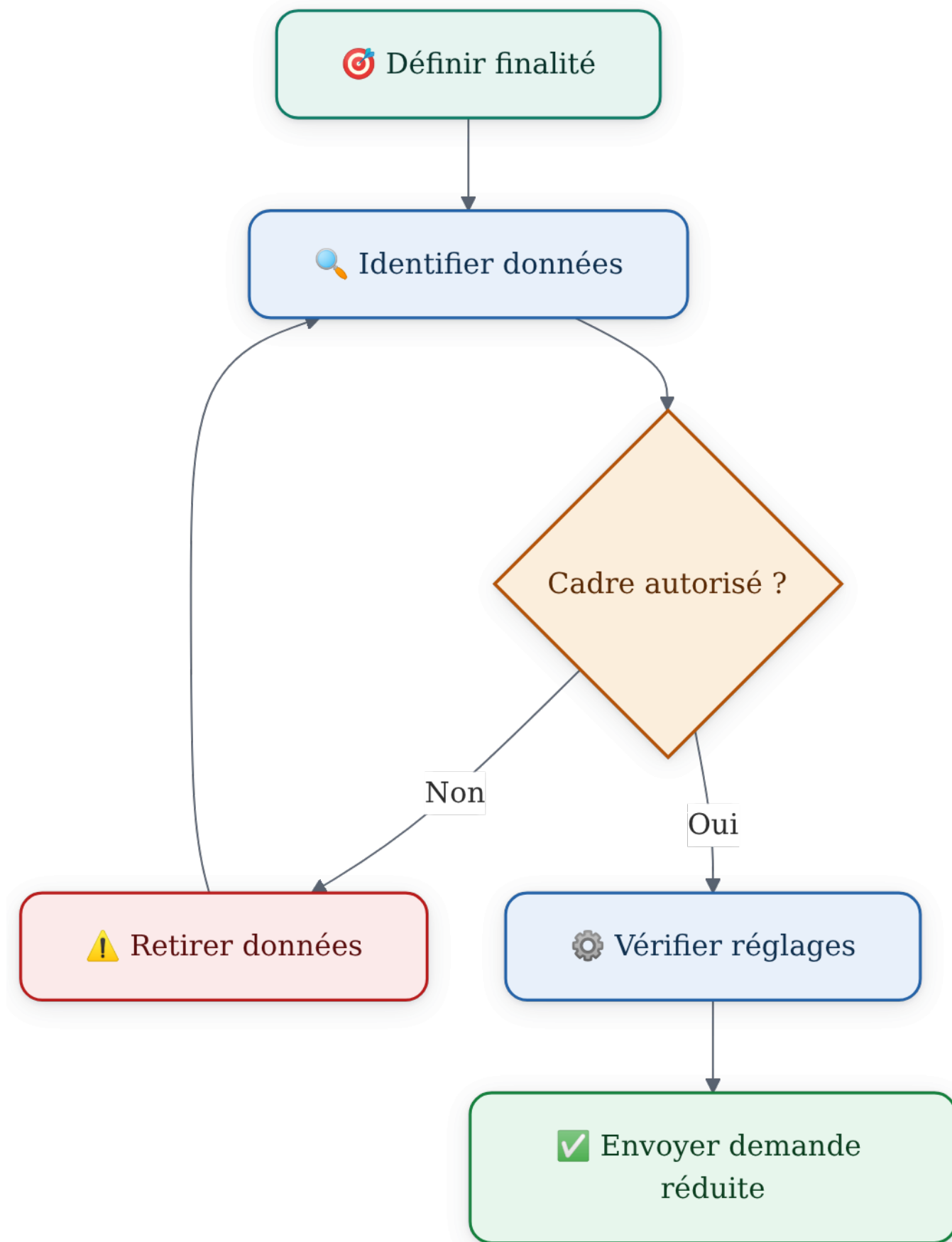
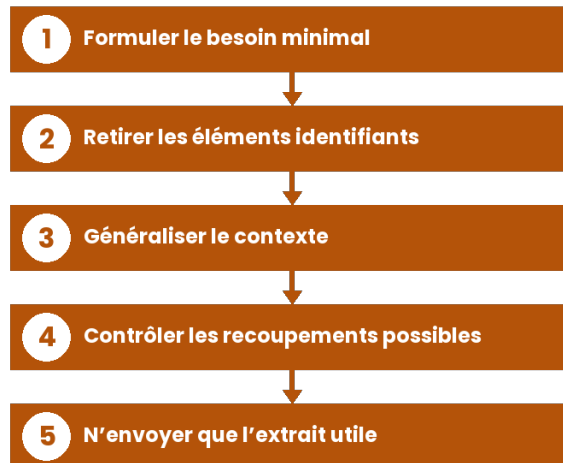


SCHÉMA Le circuit de contrôle à appliquer avant d'utiliser une IA avec un contenu réel.

3. Réduire et anonymiser avant l'envoi



1 Formuler le besoin minimal

Demandez une reformulation, un plan ou une synthèse avec le moins d'informations nécessaire.

2 Retirer les éléments identifiants

Supprimez les noms, coordonnées, identifiants, localisations précises, références de dossiers et détails inutiles.

3 Généraliser le contexte

Préférez une situation fictive ou générique lorsqu'elle permet d'obtenir la même aide.

4 Contrôler les recoupements possibles

Vérifiez que les éléments restants ne permettent pas, ensemble, de rattacher le contenu à une personne.

5 N'envoyer que l'extrait utile

Évitez le fichier complet lorsqu'un passage limité suffit à traiter la demande.

4. Vérifier l'outil et le compte

- ☐ **Consulter les informations de confidentialité du fournisseur**
Le traitement dépend du service, de l'offre choisie, des réglages et du contexte d'utilisation.
- ☐ **Vérifier la conservation des conversations et les possibilités de suppression**
- ☐ **Contrôler les réglages de confidentialité disponibles**
- ☐ **Examiner les accès accordés aux applications et connecteurs**
- ☐ **Protéger le compte utilisé**
La sécurité du compte fait partie du contrôle des données.
- ☐ **Utiliser uniquement un outil validé pour les usages professionnels ou sensibles**
Sollicitez si besoin le DPO, l'équipe sécurité, le service juridique ou le responsable métier.

Repères rapides : partager ou reformuler ?

Situation	Réflexe à adopter
Demander une reformulation	Fournir un extrait anonymisé et limité au besoin.
Résumer un document	Retirer les identifiants et ne transmettre que les passages nécessaires.
Analyser une information de santé, bancaire ou d'identité	Ne pas l'utiliser dans un outil non validé pour cet usage.
Utiliser un connecteur ou importer un fichier	Vérifier les accès accordés, le contenu partagé et le cadre du service.
Traiter une donnée professionnelle confidentielle	Appliquer les règles internes et demander une validation si nécessaire.

! Une option de confidentialité ne suffit pas à elle seule

Un réglage utile peut réduire certains risques, mais ne rend pas un contenu confidentiel sans risque. La première protection reste la minimisation des données avant tout partage.

En cas d'envoi accidentel

Agissez sans attendre : vérifiez les options de suppression disponibles, retirez les accès ou connecteurs concernés si nécessaire, puis signalez l'incident selon les procédures de votre organisation. Conservez le réflexe de ne pas répéter l'envoi avec des informations supplémentaires.

Le RGPD s'applique aux traitements de données personnelles, y compris dans les usages de systèmes d'IA. L'AI Act complète ce cadre pour les systèmes d'intelligence artificielle ; il ne remplace pas le RGPD.