

Check RGPD de vos usages d'IA

Votre rapport de conformité RGPD de vos usages d'IA

Établi le 31 octobre 2026 pour exemple.fr · Outil déclaré : Copilot Chat (gratuit)

VERDICT

Orange

41 / 100

Démarche engagée, preuves incomplètes

Le cadre existe pour vos principaux outils, mais pas pour tous les usages, ou il n'est pas assez documenté pour être démontré en cas de contrôle de la CNIL.

Vos résultats par pilier

Registre et qualification

Savoir quelles données vos usages traitent

 49 / 100

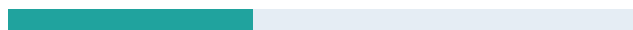
Fournisseurs

Contrats, entraînement, transferts

 28 / 100

Analyse d'impact et sécurité

Évaluer et maîtriser les risques

 39 / 100

Personnes et règles

Information, droits, règles d'usage

 49 / 100

Les écarts relevés et quoi faire

POINT CLÉ · REGISTRE ET QUALIFICATION

Les usages d'IA ne figurent pas au registre des traitements.

Inscrire chaque usage d'IA au registre (article 30) avec sa finalité, sa base légale, les données traitées et le fournisseur : c'est la première pièce que demandera la CNIL.

POINT CLÉ · FOURNISSEURS

La réutilisation de vos données par les fournisseurs d'IA n'est pas exclue ou pas vérifiée.

Vérifier pour chaque outil le contrat de sous-traitance (article 28) et désactiver toute réutilisation de vos données pour l'entraînement : sinon le fournisseur devient responsable de traitement pour son propre compte.

POINT CLÉ · ANALYSE D'IMPACT ET SÉCURITÉ

Les usages d'IA à risque ne font pas l'objet d'une analyse d'impact.

Documenter pour chaque projet si une analyse d'impact est due (données sensibles, évaluation de salariés, décision sur des personnes, grande échelle) et la mener avant le déploiement (article 35).

POINT CLÉ · PERSONNES ET RÈGLES

Les personnes concernées ne sont pas informées de l'usage de l'IA sur leurs données.

Rédiger une information claire pour chaque population (salariés, clients, candidats) : finalité, données, fournisseur, durée, droits (articles 13 et 14).

FOURNISSEURS

La localisation des données et les transferts hors UE ne sont pas documentés.

Documenter où sont traitées et conservées les données de chaque outil et sur quel fondement elles sont transférées, avec une clause de repli vers les clauses contractuelles types pour les fournisseurs américains.

ANALYSE D'IMPACT ET SÉCURITÉ

Les droits d'accès ne sont pas revus avant d'ouvrir un assistant aux documents.

Revoir le sur-partage avant toute ouverture : un assistant rend trouvable tout ce qui est accessible. Appliquer des étiquettes de sensibilité et des règles de prévention des fuites (article 32).

REGISTRE ET QUALIFICATION

Les projets d'IA ne sont pas qualifiés avec le DPO avant leur lancement.

Remplir une fiche projet d'une page avant tout lancement : données personnelles, rôles, mode de déploiement, personnes concernées, et l'IA aide, propose ou décide. Le RGPD ne connaît pas la phase pilote.

FOURNISSEURS

Les paramètres de conservation et de connexion des outils d'IA n'ont pas été vérifiés.

Fixer et documenter la durée de conservation des prompts et des journaux, les fonctions connectées (web, messagerie, agents) et les conditions d'accès du fournisseur à vos données.

PERSONNES ET RÈGLES

Les demandes de droits portant sur les données passées par l'IA ne sont pas organisées.

Écrire la procédure de traitement des droits (accès, rectification, effacement, opposition) pour les données des outils d'IA et obtenir l'assistance du fournisseur dans le contrat.

Votre plan d'action à 90 jours

- | | | |
|---|---------------|--|
| 1 | 0 à 30 jours | Traiter les écarts signalés dans ce rapport, en commençant par les points clés. |
| 2 | 31 à 60 jours | Étendre la fiche projet et le registre aux pilotes, aux agents et aux fonctions d'IA des logiciels métier. |
| 3 | 61 à 90 jours | Mettre à jour les analyses d'impact, tester la procédure de droits des personnes et programmer une revue annuelle. |

Ce que demande le RGPD

Le RGPD n'a pas de calendrier : il s'applique déjà à tout usage d'IA qui traite des données personnelles, c'est-à-dire presque tous. Il demande d'inscrire ces traitements au registre (article 30), d'encadrer les fournisseurs par contrat (article 28), d'analyser l'impact des traitements à risque (article 35), d'informer les personnes (articles 13 et 14), de garantir une intervention humaine face aux décisions automatisées (article 22) et de sécuriser les données (article 32). La CNIL a précisé sa doctrine sur l'IA en 2024 et 2025 et a placé le recrutement en tête de ses contrôles 2026. L'omnibus numérique n'est pas adopté : le RGPD s'applique tel quel, avec des amendes pouvant atteindre 4 % du chiffre d'affaires mondial.

Pour passer à l'action

Kit RGPD du commanditaire de projet IA (Word + Excel, gratuit) : les cinq questions du DPO, les six familles de projets, le fournisseur, l'analyse d'impact, les personnes. www.nextstart.ai/kit-rgpd/

Modèle de charte IA : outils autorisés, données interdites, contrôle humain. www.nextstart.ai/modele-charte-ia/

Pour cadrer vos projets avec votre DPO ou former vos équipes : Flavien Besset, 01 89 16 48 05, flavienbesset@nextstart.fr

Ce rapport est établi à partir de vos seules réponses. C'est un outil d'aide à la décision : il ne constitue pas un avis juridique.