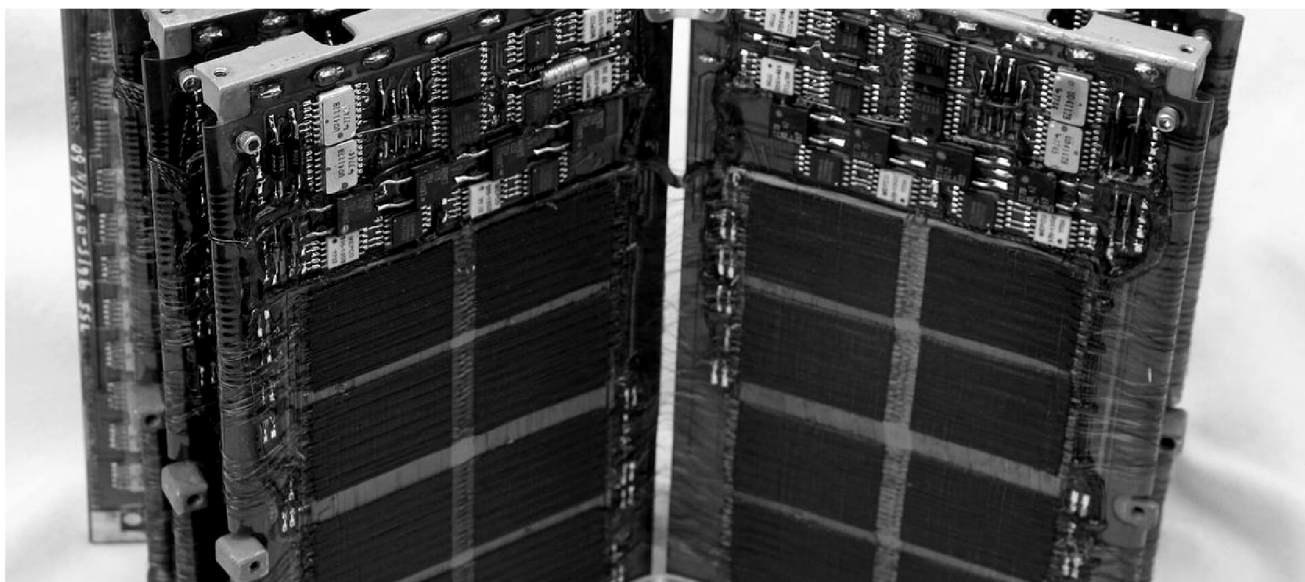


IA et RGPD : garder la main sur vos données

IA et RGPD vont de pair dès qu'un outil d'intelligence artificielle reçoit une donnée personnelle : un nom dans un prompt, un dossier joint, une messagerie connectée. Ce guide détaille ce qu'il faut vérifier avant d'utiliser ChatGPT, Claude ou Copilot, ou de lancer un projet sur mesure : données, base légale, contrat, transferts, analyse d'impact, charte et AI Act.



MÉMOIRE À TORES DE FERRITE D'UN MISSILE TITAN • STEVE JURVETSON • CC BY 2.0

- 01 IA et RGPD : ce qui s'applique dès qu'une donnée personnelle entre dans l'outil
 - 02 Partir d'un document concret pour voir les données
 - 03 Peut-on utiliser ChatGPT, Claude ou Copilot en entreprise sans enfreindre le RGPD ?
 - 04 Quelle base légale pour utiliser l'IA avec des données personnelles ?
 - 05 Dessiner le parcours complet des informations
 - 06 Responsable de traitement ou sous-traitant : qui fait quoi ?
 - 07 Transferts hors de l'Union : où en est le Data Privacy Framework ?
 - 08 Quand une analyse d'impact (AIPD) est-elle obligatoire ?
 - 09 Vos données servent-elles à entraîner les modèles ?
 - 10 Registre, durées de conservation et droits des personnes
 - 11 Comment encadrer l'usage de l'IA par vos équipes ?
 - 12 AI Act et RGPD : quelle articulation et quelles obligations ?
 - 13 IA et RGPD : notre méthode pour garder la main sur un projet
-

IA et RGPD : ce qui s'applique dès qu'une donnée personnelle entre dans l'outil

Le RGPD n'a pas de règles propres à l'intelligence artificielle : il s'applique à tout traitement de données personnelles, et un outil d'IA en devient un dès qu'il reçoit une information qui permet de reconnaître une personne. Les principes restent ceux de n'importe quel logiciel de gestion : un but défini, une base légale, des données limitées au nécessaire, une durée de conservation, la sécurité et le respect des droits. Ce qui change avec l'IA, ce sont les endroits où les données peuvent partir sans que personne n'y pense.

Trois situations reviennent. Un salarié colle un texte dans un assistant conversationnel. Un outil est connecté à la messagerie ou aux documents partagés. Une automatisation sur mesure envoie des extraits de dossiers à un modèle par API, c'est-à-dire par une interface qui permet à deux logiciels d'échanger des données. Dans les trois cas, l'entreprise qui décide de l'usage reste responsable de ce qu'elle fait des données. Le règlement européen sur l'IA, appelé AI Act, s'ajoute au RGPD sans le remplacer.

En France, la référence est la CNIL : ses questions-réponses sur l'utilisation d'une IA générative et ses fiches pratiques sur l'IA structurent ce guide. Celui-ci n'est pas un conseil juridique. Pour un traitement sensible ou à grande échelle, faites valider vos choix par votre délégué à la protection des données (DPO), la personne chargée de veiller au respect du RGPD dans l'organisation, ou par votre conseil.

Sécurité et protection des données chez Blink ➤

Partir d'un document concret pour voir les données

La façon la plus fiable de savoir quelles données personnelles partent dans un outil d'IA est de prendre un vrai exemple de la tâche et de le lire ligne par ligne. Un compte rendu, un courriel ou une fiche client contient souvent plus qu'on ne le croit : nom, téléphone, situation familiale, montant d'un litige, appréciation sur un collaborateur. Une donnée personnelle est toute information qui identifie une personne, directement ou en la recoupant avec d'autres éléments.

Classez ensuite chaque information en trois colonnes : ce qui est disponible, ce qui est réellement utile à la tâche, ce qui peut être remplacé par une information moins précise. C'est le principe de minimisation du RGPD, appliqué au prompt, c'est-à-dire à la consigne et au contenu envoyés au modèle. La CNIL recommande que chaque utilisateur ne transmette que des informations qu'il est autorisé à partager, et d'éviter autant que possible les données personnelles lorsque le modèle est appelé par API.

Retirer les noms ne rend pas un document anonyme. Remplacer une identité par un code relève de la pseudonymisation : la personne reste identifiable par celui qui détient la correspondance, et le RGPD continue de s'appliquer. L'anonymisation suppose que plus personne ne puisse raisonnablement retrouver l'identité, ce qui est difficile à atteindre avec des textes riches en détails.

Exemple illustratif : trier les demandes entrantes

Pour savoir si un message concerne une livraison, une réclamation ou une demande de devis, le corps du message suffit en général. L'historique complet du client, sa date de naissance ou ses factures n'ont pas à être transmis au modèle. On teste d'abord sur quelques messages réels si l'extrait limité donne le bon classement, puis on fige ce périmètre dans l'outil plutôt que de compter sur la discipline de chacun.

03

Peut-on utiliser ChatGPT, Claude ou Copilot en entreprise sans enfreindre le RGPD ?

Oui, si l'offre et sa configuration conviennent à l'usage prévu, et si vous pouvez le montrer avec des documents plutôt qu'avec une impression. Un même assistant existe souvent en version grand public, en offre professionnelle administrée par l'entreprise et en API pour les développeurs. L'utilisation des données, leur conservation et le contrat proposé peuvent varier d'une version à l'autre : la question n'est donc pas « cet outil est-il conforme ? », mais « cette offre, réglée ainsi, convient-elle à cet usage ? ».

Le cas le plus délicat est le compte personnel d'un salarié utilisé pour le travail : l'entreprise ne contrôle ni les réglages, ni l'historique, ni le contrat. La CNIL rappelle qu'il revient à l'organisation utilisatrice d'interroger le fournisseur sur la conformité de son système. Elle distingue aussi les modes de déploiement : une installation sur vos propres serveurs limite le risque d'extraction par un tiers, un service hébergé suppose un contrat de sous-traitance qui précise les accès autorisés. Pour comparer deux offres, posez les mêmes questions et notez où se trouve chaque réponse. Une case « à confirmer » vaut mieux qu'une promesse générale : elle montre ce qu'il reste à obtenir avant de décider.

Question à poser	Où chercher la réponse	Ce que cela change
Les contenus servent-ils à améliorer les modèles ?	Page de confidentialité de l'offre exacte, réglages administrateur	Une réutilisation par le fournisseur peut en faire un responsable de traitement pour cette partie
Combien de temps les échanges sont-ils conservés ?	Documentation de l'offre, contrat, console d'administration	Fixe la durée à inscrire au registre et à annoncer aux personnes
Un accord de sous-traitance (article 28) est-il signé ?	Contrat ou accord de traitement des données du fournisseur	Sans lui, la relation avec le fournisseur n'est pas encadrée
Où les données sont-elles traitées, et par qui ?	Liste des sous-traitants ultérieurs, options de localisation	Révèle les transferts hors de l'Union à encadrer
Qui administre les comptes et les connexions ?	Console d'administration de l'offre professionnelle	Permet de fermer un accès ou de couper un connecteur

Utiliser Claude en entreprise : le guide [➤](#)

04

Quelle base légale pour utiliser l'IA avec des données personnelles ?

Il n'existe pas de base légale propre à l'IA : elle dépend de la finalité, c'est-à-dire du but concret du traitement. L'article 6 du RGPD en prévoit six : consentement, exécution d'un contrat, obligation légale, sauvegarde des intérêts vitaux, mission d'intérêt public et intérêt légitime. Pour un usage interne, l'exécution d'un contrat ou l'intérêt légitime peuvent être envisagés selon le cas ; le consentement n'est pas la réponse par défaut. L'intérêt légitime suppose de mettre en balance votre intérêt et les attentes des personnes.

Formulez la finalité de façon vérifiable. « Utiliser l'IA pour gagner du temps » ne permet aucune analyse ; « préparer une synthèse de dossier relue par le chargé de suivi » permet de dire quelles données sont nécessaires. Si les données ont été collectées pour autre chose, par exemple la gestion d'un contrat, vérifiez que le nouvel usage reste compatible avec l'usage initial. Les données sensibles, comme la santé, les opinions ou l'appartenance syndicale, relèvent de l'article 9 et sont interdites sauf exceptions : tenez-les à l'écart des outils généralistes.

Les personnes concernées doivent être informées (articles 13 et 14) : finalités, destinataires, transferts éventuels, durées de conservation et droits. Mettez à jour votre politique de confidentialité et, pour les salariés, la note d'information interne. Une décision fondée exclusivement sur un traitement automatisé et produisant des effets importants pour la personne, comme un refus de candidature, relève en plus de l'article 22.

05

Dessiner le parcours complet des informations

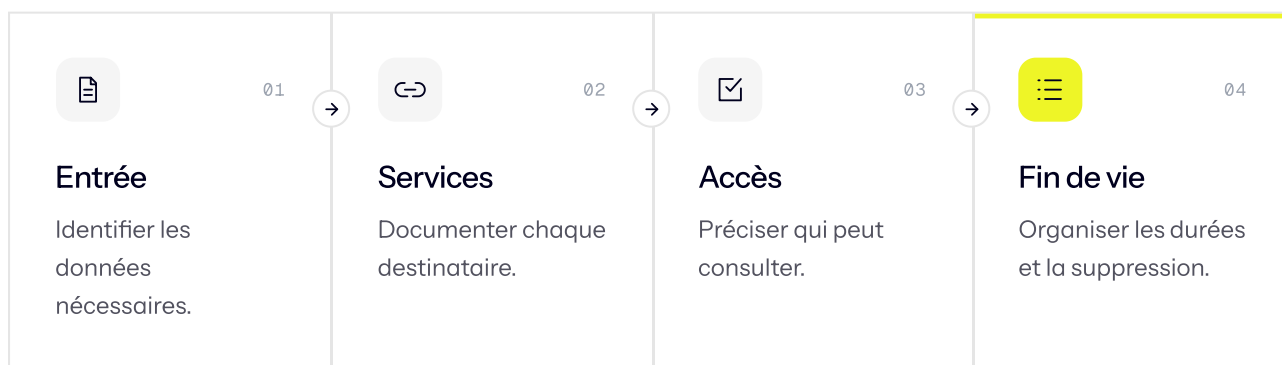
Pour garder la main, dessinez le trajet d'une donnée depuis son entrée jusqu'à sa suppression : ce qui entre, quels services la reçoivent, qui peut la consulter, combien de temps elle reste. Un projet d'IA fait souvent intervenir plusieurs acteurs : votre logiciel métier, un outil d'automatisation, le fournisseur du modèle, une base documentaire, un service de supervision. Chacun reçoit des données et doit apparaître sur le schéma avec son rôle.

Ajoutez les copies moins visibles : historiques de conversation, pièces jointes conservées, journaux d'erreur, sauvegardes. Avec un RAG, la technique qui fait chercher le modèle dans vos documents avant de répondre, l'index créé à partir de ces documents est une copie de plus. Chaque copie est un endroit où une donnée vit, peut être consultée et devra être effacée.

Un test simple vérifie que le schéma sert à agir : si une personne demande l'effacement de ses données, qui sait les retrouver à chaque étape ? Si la réponse manque pour une étape, c'est cette étape qu'il faut revoir avant la mise en service. Ce même schéma alimente ensuite le registre des traitements et, si elle est nécessaire, l'analyse d'impact.

- ✓ **Entrée** : les données réellement nécessaires à la tâche, et celles qu'on écarte.
- ✓ **Services** : chaque destinataire, son rôle et son lieu de traitement.
- ✓ **Accès** : qui peut consulter les données, côté entreprise et côté fournisseurs.
- ✓ **Fin de vie** : les durées de conservation et la procédure de suppression.

Comprendre le RAG et ses copies de documents ↗



Repère pédagogique à adapter à votre organisation.

Responsable de traitement ou sous-traitant : qui fait quoi ?

L'entreprise qui décide d'utiliser l'IA pour une finalité est en principe responsable de traitement ; le fournisseur qui traite les données pour son compte et sur ses instructions est sous-traitant au sens de l'article 28 du RGPD. Ce partage n'est pas automatique. Si le fournisseur réutilise les données pour ses propres besoins, par exemple améliorer ses modèles, il peut devenir responsable de cette partie. La fiche pratique n° 3 de la CNIL aide à qualifier les acteurs d'un système d'IA.

L'article 28 impose un contrat écrit. Beaucoup de fournisseurs le proposent sous forme d'accord de traitement des données, souvent appelé DPA. Vérifiez qu'il correspond à l'offre souscrite : un accord prévu pour l'offre entreprise ne couvre pas forcément le compte d'un salarié ouvert avec sa carte bancaire. Un intégrateur, comme une agence qui développe l'automatisation, peut lui aussi être sous-traitant s'il accède aux données. La chaîne doit alors être connue de bout en bout : qui a fait appel à qui, avec quelle autorisation, pour quelles opérations.

- ✓ Traitement uniquement sur instruction documentée du client.
- ✓ Confidentialité des personnes autorisées à traiter les données.
- ✓ Mesures de sécurité adaptées au risque.
- ✓ Recours à d'autres sous-traitants soumis à autorisation, avec information en cas de changement.
- ✓ Aide au client pour les droits des personnes, les violations et l'analyse d'impact.
- ✓ Suppression ou restitution des données en fin de prestation, et possibilité d'audit.

Transferts hors de l'Union : où en est le Data Privacy Framework ?

Un transfert de données hors de l'Union européenne est possible si le pays bénéficie d'une décision d'adéquation de la Commission ou si des garanties appropriées sont en place, comme les clauses contractuelles types. Pour les États-Unis, la décision d'adéquation du 10 juillet 2023 sur le Data Privacy Framework, le cadre de protection des données UE-États-Unis, permet de transférer des données vers les entreprises américaines qui y adhèrent.

Ce cadre a été contesté. Le Tribunal de l'Union européenne a rejeté le recours de Philippe Latombe le 3 septembre 2025 (affaire T-553/23). Un pourvoi a été formé le 31 octobre 2025 devant la Cour de justice (affaire C-703/25 P). À notre connaissance, la Cour ne s'était pas encore prononcée au 6 octobre 2026, et la décision d'adéquation restait applicable. La même Cour a déjà invalidé deux dispositifs précédents : suivez l'affaire sur le site de la Cour avant toute décision structurante.

En pratique, vérifiez que le fournisseur adhère au cadre pour les services concernés, lisez ce que couvrent ses options de localisation en Europe (stockage, traitement, assistance) et repérez ses sous-traitants situés hors de l'Union. Un accès à distance depuis un pays tiers peut aussi constituer un transfert. Prévoyez enfin une solution de repli, comme les clauses contractuelles types, si le cadre venait à tomber.

08

Quand une analyse d'impact (AIPD) est-elle obligatoire ?

Une analyse d'impact relative à la protection des données (AIPD) est obligatoire avant la mise en œuvre d'un traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes (article 35 du RGPD). Pour en juger, la CNIL renvoie aux neuf critères du comité européen de la protection des données : un traitement qui en remplit au moins deux doit en principe faire l'objet d'une AIPD. La CNIL publie aussi une liste de traitements pour lesquels elle est toujours exigée.

Plusieurs critères concernent souvent l'IA : données sensibles ou très personnelles, traitement à grande échelle, personnes vulnérables, croisement de jeux de données, usage innovant, évaluation ou notation, décision automatisée avec effet important. Un outil qui trie des candidatures ou analyse les messages des salariés en réunit vite deux. Un assistant qui reformule des textes commerciaux sans données personnelles n'en réunit aucun. Dans ses questions-réponses sur l'IA générative, la CNIL invite à associer le DPO et à envisager une AIPD dès le déploiement.

Une AIPD décrit le traitement, justifie sa nécessité et sa proportionnalité, évalue les risques pour les personnes et liste les mesures qui les réduisent. Elle se prépare bien avant le lancement, car ses conclusions peuvent changer le périmètre. Le schéma du parcours des données en fournit la base. Pour un système classé à haut risque par l'AI Act, le déployeur s'appuie aussi sur les informations que le fournisseur doit lui transmettre.

09

Vos données servent-elles à entraîner les modèles ?

Cela dépend de l'offre, du contrat et des réglages : la seule réponse fiable est celle des documents de l'offre que vous utilisez réellement. Plusieurs éditeurs distinguent leurs offres grand public, où un réglage autorise ou non l'usage des conversations pour améliorer les modèles, et leurs offres professionnelles ou leur API, présentées comme non utilisées pour l'entraînement par défaut. Ces conditions évoluent : plusieurs acteurs les ont déjà modifiées. Une vérification datée vaut mieux qu'une certitude ancienne.

Ne pas entraîner un modèle ne signifie pas ne rien conserver. Un fournisseur peut garder les échanges pendant une durée donnée, par exemple pour détecter des abus, ou les conserver

lorsque l'utilisateur envoie un avis sur une réponse. Demandez la durée de conservation et la façon de supprimer, en plus de la règle d'entraînement.

- ✓ Identifiez l'offre exacte et le type de compte : personnel, équipe, entreprise ou API.
- ✓ Lisez la page de confidentialité et l'accord de traitement propres à cette offre.
- ✓ Contrôlez les réglages de l'administrateur : entraînement, historique, conservation, connecteurs.
- ✓ Repérez les exceptions : avis envoyés par les utilisateurs, conservation pour la sécurité.
- ✓ Gardez une copie datée de ce que vous avez vérifié et refaites le contrôle au renouvellement.

10

Registre, durées de conservation et droits des personnes

Un usage de l'IA qui touche des données personnelles doit figurer dans le registre des activités de traitement prévu par l'article 30 du RGPD. La CNIL rappelle que l'obligation vise toutes les organisations. La dérogation prévue pour celles de moins de 250 salariés est très limitée : elle ne couvre pas les traitements réguliers, ceux qui présentent un risque ou ceux qui portent sur des données sensibles. Dans le doute, la CNIL recommande d'inscrire le traitement, et propose un modèle simplifié de registre.

Fixez une durée pour chaque copie : historique des conversations, résultats générés, journaux techniques, documents indexés. La règle est de conserver le temps nécessaire à la finalité, puis de supprimer ou d'archiver. Réglez la conservation dans l'outil quand il le permet ; sinon, prévoyez une purge régulière avec un responsable nommé.

Les personnes gardent leurs droits : accès, rectification, effacement, opposition, limitation et portabilité. Avec l'IA, la difficulté est pratique : retrouver les données d'une personne dans chaque outil et chaque copie. Faites un essai avant la mise en service, sur une demande fictive d'accès puis d'effacement : vous verrez vite si le parcours documenté tient.



PERFORATION DE CARTES · ARCHIVES NATIONALES AMÉRICAINES

NARA · DOMAINE PUBLIC

11

Comment encadrer l'usage de l'IA par vos équipes ?

Avec une charte d'usage courte, des outils validés et une formation adaptée au métier. La CNIL recommande des politiques internes qui définissent clairement les usages autorisés et interdits, la formation des utilisateurs à ce que les systèmes savent faire et à leurs limites, le recueil régulier de leurs retours et l'implication du DPO dès le départ.

Une interdiction générale est rarement tenue : l'usage se déplace alors vers des comptes personnels, hors de tout contrôle. Mieux vaut fournir un outil administré et dire précisément ce qu'on y met. Illustrez chaque règle par des cas du métier : un courrier à reformuler, un dossier client à résumer, une liste de candidats. Pour chacun, indiquez le circuit autorisé et la personne à contacter en cas de doute.

- ✓ Outils et comptes autorisés, et qui les administre.
- ✓ Données à ne jamais saisir hors d'un outil validé : santé, ressources humaines, données clients identifiantes.
- ✓ Vérification systématique des résultats avant tout envoi ou décision.
- ✓ Règles pour les connexions à la messagerie et aux espaces documentaires.
- ✓ Conduite à tenir en cas d'erreur ou de fuite : qui prévenir, et comment suspendre l'usage.

Former vos équipes à un usage maîtrisé de l'IA ↗

AI Act et RGPD : quelle articulation et quelles obligations ?

Les deux textes se cumulent. Le RGPD protège les données personnelles ; l'AI Act, le règlement (UE) 2024/1689, encadre les systèmes d'IA selon leur niveau de risque, même sans données personnelles, et précise qu'il n'affecte pas le RGPD. Il distingue le fournisseur, qui développe ou met un système sur le marché, et le déployeur, qui l'utilise sous sa propre autorité à titre professionnel. La plupart des entreprises qui adoptent ChatGPT, Claude ou Copilot sont des déployeurs.

L'article 4 porte sur la maîtrise de l'IA, applicable depuis le 2 février 2025. Le règlement (UE) 2026/1744, dit « omnibus numérique sur l'IA », publié au Journal officiel le 24 juillet 2026 et entré en vigueur le 27 juillet 2026, l'a réécrit : fournisseurs et déployeurs prennent des mesures pour favoriser la maîtrise de l'IA de leur personnel, sans être tenus de garantir un niveau donné pour chaque personne. Aucun format de formation ni volume d'heures n'est imposé.

Ce même règlement a reporté les obligations des systèmes à haut risque. Une autre proposition, l'omnibus numérique présenté par la Commission le 19 novembre 2025, vise notamment à modifier le RGPD. Nous n'avons pas pu confirmer son adoption au 6 octobre 2026 : vérifiez son état sur le site de la Commission ou sur EUR-Lex avant d'en tenir compte.

Niveau de risque	Exemples	Pour l'entreprise utilisatrice (déployeur)	Application
Pratiques interdites	Notation sociale, reconnaissance des émotions au travail	Ne pas les utiliser	Depuis le 2 février 2025 ; interdictions ajoutées par l'omnibus au 2 décembre 2026
Haut risque (annexe III)	Tri de candidatures, évaluation de salariés, notation de crédit, éducation	Suivre la notice, surveillance humaine par des personnes compétentes, conservation des journaux, information des salariés	2 décembre 2027
Haut risque intégré à un produit (annexe I)	Machines, jouets, dispositifs médicaux	Obligations surtout pour les fabricants et fournisseurs	2 août 2028
Transparence (article 50)	Agent conversationnel, contenus truqués, textes publiés sur des sujets d'intérêt public	Signaler les hypertrucages et les textes publiés pour informer le public, informer les personnes en cas de reconnaissance des émotions ; l'information sur le dialogue avec une IA est prévue par le fournisseur	Depuis le 2 août 2026
Risque minimal	Filtre anti-spam, aide à la rédaction interne	Pas d'obligation spécifique, en dehors de l'article 4	Sans objet

Agents IA : ce qu'ils peuvent faire et sous quel contrôle ↗

13

IA et RGPD : notre méthode pour garder la main sur un projet

Chez Blink, nous préférons une description composant par composant à une étiquette. Dire « conforme » ou « souverain » sans décrire les flux et les accès ne donne à votre DPO rien à examiner. Au cadrage, nous partons d'un dossier réel, listons les données utiles à chaque étape et nommons chaque service avec son rôle. Nous définissons avec vous les lieux d'hébergement et les services autorisés, et les éventuels transferts ou appels à des services externes sont identifiés avant activation.

L'automatisation est ensuite écrite pour vous et branchée sur vos outils existants : elle n'envoie au modèle que les champs retenus au cadrage, ce qui fait de la minimisation une propriété du code plutôt qu'une consigne. Les conditions d'utilisation des données par chaque service d'IA sont vérifiées pour la configuration retenue. Sur votre portail, l'équipe voit ce qui tourne et valide avant ce qui part ; la validation humaine porte sur les actions et droits convenus au cadrage.

Les modalités d'export, de conservation, de suppression et de sauvegarde sont documentées avant livraison. Le suivi mensuel permet de revoir ce qui a bougé : conditions d'un fournisseur, nouvelle obligation, nouvel usage. La qualification juridique et l'AIPD restent l'affaire de votre organisation et de son DPO ; notre rôle est de leur fournir une description exacte du fonctionnement.

[Cartographier vos processus avant d'automatiser ↗](#)

[Le portail Blink : voir ce qui tourne et valider ↗](#)

Sources et repères

CNIL : questions-réponses sur l'utilisation d'un système d'IA générative

CNIL : les fiches pratiques IA

CNIL : réaliser une analyse d'impact si nécessaire (fiche IA n° 5)

CNIL : le registre des activités de traitement

EUR-Lex : règlement (UE) 2026/1744, omnibus numérique sur l'IA

Commission européenne : législation sur l'IA et calendrier d'application

Commission européenne : transferts de données UE-États-Unis

EUR-Lex : pourvoi C-703/25 P contre l'arrêt T-553/23 (Data Privacy Framework)

QUESTIONS

Questions fréquentes

Votre question n'y est pas ? Posez-la pendant l'échange gratuit de trente minutes.

01 **L'IA est-elle compatible avec le RGPD ?**

Oui. Le RGPD n'interdit pas l'intelligence artificielle : il encadre les données personnelles qu'elle traite. Un usage est compatible s'il a un but précis, une base légale, des données limitées au nécessaire, une durée de conservation, un contrat avec les fournisseurs et des personnes informées. La difficulté tient surtout à la multiplication des services et des copies, qu'il faut connaître pour pouvoir répondre d'un usage.

02 **Peut-on mettre des données clients dans ChatGPT ?**

Pas dans un compte personnel non encadré. Avec une offre professionnelle administrée, un accord de sous-traitance, des réglages vérifiés et une finalité inscrite au registre, c'est envisageable pour les données réellement utiles. Retirez ce qui n'est pas nécessaire, évitez les données sensibles et vérifiez ce que l'offre prévoit pour la conservation et l'entraînement.

03 **ChatGPT est-il conforme au RGPD ?**

La question se pose plutôt pour votre usage. Un même outil existe en versions grand public, professionnelle et API, avec des conditions différentes. La CNIL invite l'organisation utilisatrice à interroger le fournisseur sur la conformité de son système. Ce qui compte : l'offre souscrite, ses réglages, le contrat, les transferts et ce que vos équipes y saisissent.

04 **Faut-il une AIPD pour utiliser ChatGPT ou Copilot ?**

Pas systématiquement. L'analyse d'impact est obligatoire si le traitement présente un risque élevé, par exemple s'il croise données sensibles et grande échelle, ou évalue des personnes. Rédiger des textes génériques sans données personnelles n'en demande pas. Analyser les messages des salariés ou trier des candidatures, probablement si. La CNIL recommande d'associer le DPO dès le déploiement.

05 **Faut-il informer ses clients que l'on utilise l'IA ?**

Si leurs données personnelles sont traitées par un outil d'IA, l'information RGPD doit couvrir la finalité, les destinataires, dont les fournisseurs, les éventuels transferts et la durée de conservation. Côté AI Act, l'article 50 impose au fournisseur de concevoir un système destiné à dialoguer avec des personnes, comme un agent conversationnel, pour qu'elles sachent qu'elles échangent avec une IA, sauf si c'est évident. Le déployeur, c'est-à-dire l'entreprise qui utilise le système, a ses propres obligations pour la reconnaissance des émotions, les hypertrucages et les textes publiés pour informer le public. Une entreprise qui fait développer son propre agent et le met en service sous son nom peut aussi être fournisseur.

06 **Faut-il le consentement des personnes pour utiliser l'IA ?**

Pas forcément. Le consentement n'est qu'une des six bases légales du RGPD. Selon la finalité, l'exécution d'un contrat ou l'intérêt légitime peuvent convenir, à condition d'en documenter l'analyse. Le consentement devient délicat quand la personne n'est pas libre de refuser, par exemple un salarié face à son employeur.

07 **Une PME doit-elle tenir un registre des traitements pour l'IA ?**

Oui, dans la grande majorité des cas. La dérogation pour les structures de moins de 250 salariés ne s'applique pas aux traitements réguliers, à risque ou portant sur des données sensibles, et un usage quotidien de l'IA sur des dossiers clients est régulier. La CNIL propose un modèle de registre simplifié pour les petites structures.

08 **L'AI Act oblige-t-il à former ses salariés à l'IA ?**

L'article 4 demande aux entreprises qui utilisent des systèmes d'IA de prendre des mesures pour favoriser la maîtrise de l'IA de leur personnel. Depuis sa modification par le règlement (UE) 2026/1744, il précise qu'aucun niveau individuel n'est à garantir. Aucun format ni volume de formation n'est imposé : une formation ciblée sur les outils réellement utilisés est une mesure cohérente.

09 **Enlever les noms suffit-il à anonymiser un document ?**

Rarement. Une fonction, une date, un lieu ou un détail de dossier peuvent suffire à reconnaître quelqu'un. Remplacer un nom par un code relève de la pseudonymisation : les données restent personnelles et le RGPD s'applique. L'anonymisation suppose que l'identification ne soit plus raisonnablement possible, ce qui se vérifie au cas par cas.

ET MAINTENANT ?

Ce guide pose les bases. Votre cas mérite trente minutes.

Le premier échange avec Blink est gratuit et sans engagement : trente minutes en visio pour examiner une tâche de votre équipe et ce qu'elle demanderait vraiment.

fr-blink.com/contact
contact@fr-blink.com

BLINK · PAUL ROBERT ET BASTIEN DOUBLET · AUTOMATISATIONS ET AGENTS IA SUR MESURE, PARTOUT EN FRANCE