bonbay ACADÉMIE

RGPD et IA, les règles essentielles

Support complet du cours

Le cours écrit de chaque leçon, avec ses schémas, ses tableaux et ses demandes à recopier, les erreurs fréquentes, l'exercice à faire sur votre poste et les points à retenir. Les entraînements et tous les corrigés sont dans le cahier d'exercices, les exemples racontés de bout en bout dans le recueil d'exemples pratiques ; les vidéos et les quiz restent sur le site du cours.

8
leçons

3
modules

4 h 40
de travail environ

Contenu mis à jour le 19 novembre 2026. Les offres et les réglages de confidentialité des éditeurs d'IA évoluent, comme les recommandations de la CNIL et les lignes directrices de la Commission européenne : vérifiez-les à la source avant de vous y fier. Ce cours ne remplace pas l'avis d'un juriste ou de votre délégué à la protection des données.

Sommaire

Module 1 Les données que vous confiez à une IA

Reconnaître une donnée personnelle ou sensible dans ce que vous envoyez, et la retirer ou la masquer avant qu'elle parte.

1	Ce qui devient une donnée personnelle quand vous écrivez à une IA	35 min
2	Anonymiser ou pseudonymiser une demande et un fichier avant de les envoyer	31 min

Module 2 Choisir ses outils et tenir ses obligations

Choisir une offre dont le contrat et les réglages conviennent, puis inscrire l'usage au registre et prévenir les personnes concernées.

3	Choisir une offre d'IA selon l'entraînement, la conservation, le contrat et l'hébergement	32 min
4	Inscrire un usage de l'IA au registre et informer les personnes concernées	32 min

Module 3 L'AI Act, la charte et les incidents

Savoir ce que l'AI Act demande à une entreprise qui utilise l'IA, écrire la charte de l'équipe, et réagir à une demande de droits ou à une fuite.

5	Ce que l'AI Act demande à une PME qui utilise l'IA, de la formation au recrutement	38 min
6	Écrire la charte d'usage de l'IA de l'entreprise et la faire vivre	34 min
7	Répondre à une demande d'exercice de droits et réagir à une fuite de données	36 min
8	Votre plan sur 30 jours et l'évaluation finale	42 min

01

Les données que vous confiez à une IA

Reconnaître une donnée personnelle ou sensible dans ce que vous envoyez, et la retirer ou la masquer avant qu'elle parte.

1 Ce qui devient une donnée personnelle quand vous écrivez à une IA

2 Anonymiser ou pseudonymiser une demande et un fichier avant de les envoyer

Leçon 1 | 35 min | Accès libre

Ce qui devient une donnée personnelle quand vous écrivez à une IA

> Une donnée personnelle est toute information qui permet de reconnaître une personne, directement ou par recoupement : un nom, mais aussi un poste rare ou une date d'arrêt. Avant d'écrire à une IA, vous repérez ce qui part, vous classez chaque élément en vert, orange ou rouge, et vous retirez ce dont la tâche n'a pas besoin.

Objectifs

- Reconnaître une donnée personnelle, une donnée sensible (article 9) et une donnée d'infraction (article 10) dans un courriel, un tableau ou un compte rendu
- Repérer tout ce qui part vers l'IA avec une demande : texte collé, pièce jointe, mémoire, connecteur
- Appliquer les principes de l'article 5 du RGPD avant d'envoyer, en retirant ce dont la tâche n'a pas besoin

Le cours

Mardi, 17 h 40, au cabinet de recrutement de Mérignac. Sophie, chargée de recrutement, doit envoyer avant le soir une synthèse de candidature à un client. Elle a sous les yeux le CV du candidat et ses notes d'entretien, qui mentionnent un arrêt maladie de trois mois l'an dernier. Elle ouvre l'assistant d'IA et s'apprête à tout coller. Avant qu'elle clique, une seule question vaut pour toute cette leçon, et pour tout le cours : **qu'est-ce qui part, chez qui, pour quoi faire, et qui le sait ?**

Cette leçon vous apprend à répondre à la première partie de la question, « qu'est-ce qui part », avant chaque envoi : reconnaître une donnée personnelle, une donnée sensible, une donnée d'infraction, et voir tout ce qui accompagne une demande. Chaque règle cite l'article qui la fonde. Ce cours explique le droit, il ne remplace pas l'avis d'un juriste ou de votre délégué à la protection des données sur un cas précis.

Ce que le RGPD appelle une donnée personnelle

L'article 4, point 1, du RGPD définit la donnée personnelle comme « toute information se rapportant à une personne physique identifiée ou identifiable ». Identifiable veut dire reconnaissable **directement ou indirectement** : par un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou par un ou plusieurs éléments propres à son identité physique, économique, culturelle ou sociale. La définition ne s'arrête donc pas au nom. Une adresse de courriel professionnelle, une plaque d'immatriculation, un numéro de client, une voix enregistrée ou une photo sont des données personnelles. Un ensemble de détails anodins aussi, dès qu'il ne correspond qu'à une personne : « la

responsable comptable arrivée en janvier » dans un cabinet de 22 personnes désigne quelqu'un aussi sûrement que son nom.

> **Anonyme pour vous, reconnaissable pour le lecteur**
>
> Le bon test n'est pas « ai-je retiré le nom ? » mais « un collègue, un client ou un proche de cette personne la reconnaîtrait-il en lisant ? ». Dans une PME de 9 personnes, « la chargée de recrutement en temps partiel » est une personne. Le recoupement se fait avec ce que le lecteur sait déjà, pas seulement avec ce qui est écrit.

Les données sensibles et les données d'infraction

L'article 9 du RGPD isole des « catégories particulières », que le cours appelle données sensibles : les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données génétiques, les données biométriques servant à identifier une personne de façon unique, les données de santé, la vie sexuelle ou l'orientation sexuelle. Leur traitement est **interdit**, sauf exceptions limitativement énumérées : consentement explicite, obligations du droit du travail et de la sécurité sociale, médecine du travail, défense d'un droit en justice, entre autres. Ces exceptions couvrent le dossier que la DRH tient pour gérer un arrêt de travail ; elles ne couvrent pas le fait de coller ce dossier dans un assistant pour gagner dix minutes. Une mention d'arrêt maladie, une reconnaissance de handicap, un mandat syndical ou un régime alimentaire lié à une religion sont des données sensibles, même noyés dans un compte rendu.

L'article 10 encadre à part les données relatives aux condamnations pénales et aux infractions : leur traitement ne se fait que sous le contrôle de l'autorité publique ou si la loi l'autorise avec des garanties. Dans une PME, elles apparaissent plus souvent que prévu : l'avis de contravention d'un véhicule de société et la désignation du conducteur, la mention d'une suspension de permis dans un dossier de chauffeur, un extrait de casier judiciaire demandé pour un poste. Enfin, certaines données ne sont pas sensibles au sens du texte mais font des dégâts si elles fuient : le **numéro de sécurité sociale**, qui suit une personne toute sa vie, l'**IBAN**, qui sert aux fraudes au virement, le salaire nominatif, l'évaluation annuelle, l'adresse personnelle, les données d'un mineur. Le cours les range avec les données sensibles, en rouge.

Le classement de ce que vous vous apprêtez à envoyer

Part tel quel

- Les informations publiques de l'entreprise : offre, tarifs affichés, plaquette
- Des chiffres agrégés : chiffre d'affaires d'un trimestre, nombre de candidatures par mois
- Un texte sans personne reconnaissable : une procédure, une fiche produit

Part réduit au nécessaire

- Nom, prénom, courriel, téléphone d'un client ou d'un candidat
- Poste, parcours, ancienneté, échanges commerciaux
- Un détail qui permet de reconnaître quelqu'un dans une petite équipe

Ne part pas

- Santé, opinions, religion, syndicat, orientation sexuelle (article 9)
- Condamnations et infractions (article 10)
- Numéro de sécurité sociale, IBAN, salaire nominatif, données d'un mineur

Le vert part tel quel, l'orange part réduit au strict nécessaire, le rouge ne part pas dans une IA.

Dix éléments de trois documents courants, classés avant envoi

Élément	Document	Catégorie	Conduite avant d'écrire à une IA
Nom et prénom du candidat	Courriel de candidature	Donnée personnelle	Orange : remplacer par [Candidat A]
Adresse de courriel et téléphone	Courriel de candidature	Donnée personnelle	Orange : retirer, la tâche n'en a pas besoin
« Reconnu travailleur handicapé, je souhaite un poste adapté »	Courriel de candidature	Donnée sensible, santé (article 9)	Rouge : retirer
Raison sociale et adresse du client professionnel	Facture	Donnée d'entreprise, sauf entreprise individuelle	Vert pour une société ; orange pour un artisan en nom propre
IBAN du client	Facture	Donnée à risque	Rouge : retirer
Montant total hors taxe	Facture	Donnée d'entreprise	Vert, sauf si elle se rattache à un particulier nommé

Élément	Document	Catégorie	Conduite avant d'écrire à une IA
Note de 2 sur 4 au critère « autonomie »	Compte rendu d'entretien annuel	Donnée personnelle, évaluation	Rouge si le salarié est nommé ou reconnaissable
« Absente six semaines au printemps pour une opération »	Compte rendu d'entretien annuel	Donnée sensible, santé (article 9)	Rouge : retirer
« Élue au CSE depuis 2025 »	Compte rendu d'entretien annuel	Donnée sensible, appartenance syndicale ou mandat (à traiter comme telle)	Rouge : retirer
Objectifs de l'année : « ouvrir deux comptes dans le Lot-et-Garonne »	Compte rendu d'entretien annuel	Donnée personnelle par rattachement	Orange : garder si le salarié est remplacé par une étiquette

Ce qui part quand vous écrivez à une IA

Une demande envoyée à un assistant d'IA ne se limite pas au texte que vous tapez. Partent aussi le texte collé, avec tout ce qu'il contient, et les pièces jointes, en entier : les colonnes masquées d'un tableur, les commentaires et le suivi des modifications d'un document Word, l'auteur inscrit dans les propriétés du fichier. Selon les réglages, l'outil garde une **mémoire** de ce que vous lui avez dit dans d'autres conversations et un **historique** conservé chez l'éditeur. Enfin, un **connecteur** ouvert vers la messagerie ou le drive laisse l'IA lire ce dont elle a besoin pour répondre, ce qui peut dépasser de loin votre question : chercher « les retours du salon » dans une boîte de réception fait remonter des signatures, des numéros et des pièces jointes de dizaines de personnes.

Tout ce qui part quand vous envoyez une demande

La consigne
Ce que vous écrivez vous-même : « Résume ces notes pour le client ».

Le texte collé
Le courriel, le compte rendu ou le tableau copié dans le champ de saisie, avec tout ce qu'il contient.

La pièce jointe
Le fichier entier : colonnes masquées, commentaires, suivi des modifications, propriétés du document.

La mémoire et l'historique
Ce que l'outil a retenu de vos conversations précédentes et ce qu'il garde dans l'historique.

Le connecteur
Ce que l'IA lit dans la messagerie, le drive ou l'agenda que vous lui avez ouverts, au-delà de votre question.

Le texte que vous tapez n'est que la couche du haut. Chaque couche peut porter des données personnelles.

> **Le fichier part en entier, la question non**
>
> Avant de joindre un tableur, copiez seulement les colonnes utiles dans un fichier neuf. Avant de joindre un document Word, acceptez ou refusez les modifications suivies et supprimez les commentaires. La leçon « Anonymiser ou pseudonymiser une demande et un fichier avant de les envoyer » montre ces gestes pas à pas, outil par outil.

Six gestes tirés de l'article 5

1. Limitation des finalités : savoir pourquoi vous envoyez. Les données d'un candidat collectées pour un poste ne servent pas à construire un « profil idéal » réutilisé pour tous les recrutements.
2. Minimisation : n'envoyer que ce que la tâche exige. Rédiger une relance de facture ne demande ni l'IBAN ni l'adresse personnelle du client.
3. Exactitude : relire ce que l'IA écrit sur une personne. Elle peut attribuer un diplôme, une date ou un propos qui n'existe pas ; rien ne part chez un client sans vérification.

4. Limitation de la conservation : ne pas laisser dormir dans l'historique une conversation qui contient des données personnelles, et régler la durée de conservation de l'outil.
5. Intégrité et confidentialité : un compte professionnel protégé, jamais un compte partagé, jamais un lien public vers une conversation qui cite quelqu'un.
6. Responsabilité : pouvoir montrer ce qui a été décidé, dans le registre et la charte d'usage, le jour où un candidat, un client ou la CNIL le demande.

Reste la base légale de l'article 6 : contrat, obligation légale, intérêt légitime, consentement, entre autres. L'usage d'une IA s'inscrit dans un traitement qui a déjà la sienne (le recrutement, la gestion des clients, la paie) ; il n'en crée pas une nouvelle. Il doit rester dans la finalité de ce traitement, et les personnes doivent en être informées, ce que traite la leçon « Inscrire un usage de l'IA au registre et informer les personnes concernées ». Si vous hésitez sur la base légale d'un usage précis, la question se pose à votre délégué à la protection des données ou à votre juriste, avant le premier envoi.

Puis-je coller ce texte

1 **Le texte est-il exempt de nom, de courriel, de téléphone, d'adresse et de numéro de dossier ?**

Non — Remplacez chaque identifiant par une étiquette, [Candidat A] ou [Client 3].

2 **Est-il exempt de tout détail qui ferait reconnaître quelqu'un par un collègue ?**

Non — Généralisez ou retirez le détail : le poste unique, la date précise, l'âge exact.

3 **Est-il exempt de santé, d'opinion, de religion, de syndicat, de condamnation, d'IBAN ou de numéro de sécurité sociale ?**

Non — Retirez ces éléments : la tâche s'en passe presque toujours.

Oui à tout — **Envoyez-le à l'outil professionnel de l'entreprise, puis relisez la réponse avant de l'utiliser.**

Trois « oui » : le texte peut partir vers l'outil professionnel de l'entreprise. Un « non » : vous retirez d'abord.

Faire travailler l'IA sans lui confier les données

Demande à recopier **Faire repérer ce qui identifie encore dans un texte déjà pseudonymisé**

```
Tu aides une PME à vérifier qu'un texte ne permet plus de reconnaître une personne avant qu'il soit partagé.
Voici un texte dont les noms, courriels et téléphones ont déjà été remplacés par des étiquettes entre crochets : [collez le texte pseudonymisé].
Relis ce texte et liste les informations qui permettraient encore d'identifier une personne, seules ou recoupées : poste unique, date précise, âge exact, lieu, événement rare, donnée de santé, opinion, mandat, condamnation.
Pour chaque information, donne : la citation exacte, la raison pour laquelle elle identifie ou expose la personne, une formulation plus générale ou la mention « à retirer ».
Ne recopie aucune autre partie du texte et ne fais aucune hypothèse sur l'identité des personnes.
```

Ce que vous devez obtenir : Une liste numérotée de trois à huit citations, chacune avec sa raison et sa reformulation : « cheffe d'atelier depuis mars 2024 » devient « encadrante d'équipe », « 58 ans » devient « plus de 50 ans », « arrêt du 4 au 18 » est à retirer (santé). Vous décidez vous-même de chaque correction.

Note : Cette demande ne s'adresse qu'à un texte DÉJÀ pseudonymisé, et à l'outil professionnel de l'entreprise. Coller le texte brut pour que l'IA y trouve les données, c'est déjà les lui envoyer.

Demande à recopier **Dresser, sans aucune donnée réelle, la liste des données d'un service**

```
Tu aides le responsable d'un service à préparer les règles d'usage de l'IA de son équipe.
Notre service : [nom du service], dans une entreprise de [effectif] personnes, secteur [secteur]. Nos tâches courantes : [liste des tâches, sans aucun nom de personne].
Dresse un tableau des catégories de données personnelles que ce service manipule probablement, avec quatre colonnes : catégorie (exemple : coordonnées de clients), documents où elle apparaît, classement (vert, orange ou rouge selon cette règle : rouge pour les données sensibles de l'article 9 du RGPD, les infractions de l'article 10, le numéro de sécurité sociale, l'IBAN, le salaire nominatif et les données de mineurs ; orange pour les autres données personnelles ; vert pour les données sans personne reconnaissable), conduite avant d'envoyer à une IA.
Signale par « à vérifier » toute catégorie dont tu n'es pas sûr qu'elle existe dans ce service.
```

Ce que vous devez obtenir : Un tableau de huit à quinze lignes, par exemple « coordonnées de clients, devis et factures, orange, remplacer par un numéro de client » ou « motifs d'absence, tableau des congés, rouge, ne jamais envoyer ». Les « à vérifier » se règlent avec l'équipe ; le tableau devient la partie « données » de votre charte.

Ce que recommande la CNIL

Dans ses questions-réponses du 18/07/2024 sur l'utilisation d'un système d'IA générative, la Commission nationale de l'informatique et des libertés recommande de ne jamais partager de données personnelles ou confidentielles avec un service grand public, de ne saisir que les informations que l'utilisateur est autorisé à partager et de prévoir des modèles de demandes validés. Les deux demandes ci-dessus en sont deux exemples.

Les erreurs fréquentes

L'erreur, et pourquoi elle coûte	La correction
Retirer le nom et penser que le texte est devenu anonyme. L'article 4 vise aussi la personne identifiable indirectement. Dans une PME, un poste, une date d'arrivée ou un événement suffit à la reconnaître pour un collègue ou un client.	Relisez le texte comme quelqu'un qui connaît l'entreprise : généralisez le poste, la date, l'âge, et retirez le détail rare. La leçon « Anonymiser ou pseudonymiser une demande et un fichier avant de les envoyer » en donne la méthode.
Joindre le fichier complet « pour que l'IA ait le contexte ». Le fichier part en entier : colonnes masquées, onglets oubliés, commentaires, suivi des modifications, auteur dans les propriétés. L'IA reçoit bien plus que la question n'en demande.	Copiez dans un fichier neuf les seules colonnes ou parties utiles, remplacez les noms par des étiquettes, puis joignez ce fichier-là.
Laisser une mention de santé dans un texte parce que « c'est pour bien faire » ou parce que l'entreprise a le droit de la connaître. Les exceptions de l'article 9 permettent à l'employeur de gérer un arrêt de travail ; elles ne couvrent pas l'envoi de cette information à un assistant d'IA pour rédiger un texte qui n'en a pas besoin.	Retirez toute donnée sensible avant d'écrire, ou remplacez-la par une formulation générale (« absence de longue durée »), et gardez le détail dans le dossier.
Oublier la mémoire et les connecteurs de l'outil. Une information donnée une fois peut être retenue et resservir dans une autre conversation, et un connecteur laisse l'IA parcourir une boîte de réception ou un drive bien au-delà de la question posée.	Consultez ce que la mémoire a retenu et effacez ce qui vise une personne, n'ouvrez un connecteur que pour une tâche précise, et limitez la recherche dans la demande elle-même.

Exercice : Trier le courriel d'un client du cabinet comptable

Julien, collaborateur comptable du cabinet d'expertise comptable de Libourne (22 personnes), reçoit le courriel ci-dessous d'un client, gérant d'une boulangerie de 6 salariés. Il veut demander à l'assistant d'IA professionnel du cabinet un brouillon de réponse qui explique la marche à suivre. Le courriel : « Bonjour Julien, ma vendeuse Camille Martin (camille.martin@exemple.fr, 06 00 00 00 41) est en arrêt maladie depuis le 3 novembre, elle m'a dit qu'elle était enceinte et qu'elle ne reviendrait sans doute qu'en avril. Elle a changé de banque, son nouvel IBAN est FR76 0000 0000 0000 0000 0000 000. Pouvez-vous corriger sa fiche de paie d'octobre, où il manque ses 4

heures supplémentaires, et me dire comment je la remplace pendant son absence ? Je pense prendre en CDD le fils de mon voisin, qui a 17 ans. Merci, Bernard, Boulangerie du Marché. » Classez chaque élément, décidez ce qui part et écrivez la demande à envoyer.

1. Relevez chaque élément qui se rapporte à une personne : identité, coordonnées, santé, banque, âge, paie.
2. Classez chacun en vert, orange ou rouge, avec l'article qui fonde le rouge quand il y en a un.
3. Décidez de ce dont le brouillon de réponse a réellement besoin pour expliquer la marche à suivre.
4. Réécrivez la situation en quelques lignes, sans aucun élément rouge et avec des étiquettes à la place des noms.
5. Écrivez la demande complète à l'assistant professionnel du cabinet.

Le corrigé est dans le cahier d'exercices et sur la page de la leçon.

À retenir

- Une donnée personnelle est toute information qui permet de reconnaître une personne, directement ou par recoupement : le nom n'est qu'un cas parmi d'autres (article 4).
- Santé, origine, opinions, religion, syndicat, génétique, biométrie, vie et orientation sexuelles sont des données sensibles (article 9) ; avec les infractions (article 10), l'IBAN, le numéro de sécurité sociale, le salaire nominatif et les données de mineurs, elles ne partent pas dans une IA.
- Une demande emporte aussi le texte collé, les pièces jointes en entier, la mémoire, l'historique et ce que lit un connecteur.
- La minimisation se pratique avant chaque envoi : la tâche dit ce dont l'IA a besoin, le reste reste chez vous.
- L'usage d'une IA s'inscrit dans un traitement qui a déjà sa base légale ; il n'en crée pas une et doit rester dans sa finalité.

Leçon 2 | 31 min | Accès libre

Anonymiser ou pseudonymiser une demande et un fichier avant de les envoyer

> Anonymiser rend toute identification impossible de façon irréversible et fait sortir la donnée du RGPD ; pseudonymiser remplace les noms par des étiquettes, garde une table de correspondance et laisse la donnée personnelle. Avant d'envoyer un texte ou un fichier à une IA, cinq gestes réduisent le risque, faits sur votre poste et non par l'IA elle-même.

Objectifs

- Distinguer l'anonymisation de la pseudonymisation et dire laquelle des deux vous avez faite
- Pseudonymiser un texte ou un tableur en cinq gestes, la table de correspondance gardée hors de l'IA
- Vérifier qu'un texte ou un fichier préparé ne permet plus de reconnaître une personne avant de l'envoyer

Le cours

Au cabinet d'expertise comptable de Libourne, Julien doit analyser le relevé des impayés d'un client, un négociant en vins : 46 factures, avec le nom des débiteurs, leurs adresses et leurs téléphones. À l'agence de communication des Chartrons, Léa a reçu les 180 réponses libres d'un questionnaire de satisfaction, signées et parfois très personnelles. Tous deux veulent l'aide d'une IA. La question du cours, « qu'est-ce qui part, chez qui, pour quoi faire, et qui le sait ? », reçoit ici sa réponse la plus concrète : ce qui part, c'est un texte ou un fichier que vous avez préparé, et dont vous savez dire s'il est anonymisé ou seulement pseudonymisé.

Deux opérations que tout oppose

La Commission nationale de l'informatique et des libertés (CNIL) définit l'**anonymisation** comme un traitement qui rend impossible, en pratique, toute identification de la personne, par quelque moyen que ce soit, et de manière irréversible. Une donnée réellement anonymisée n'est plus une donnée personnelle : le RGPD ne s'y applique plus. La **pseudonymisation**, définie à l'article 4, point 5, du RGPD, fait en sorte que les données ne puissent plus être attribuées à une personne précise sans informations supplémentaires, conservées séparément et protégées. Elle se défait avec la table de correspondance : la donnée reste personnelle, et le RGPD s'applique entièrement. L'article 32 la cite, avec le chiffrement, parmi les mesures de sécurité adaptées au risque. Retenez l'ordre de grandeur : avant un envoi à une IA, vous faites presque toujours une pseudonymisation. C'est utile, ce n'est pas une sortie du RGPD.

Anonymiser et pseudonymiser ne protègent pas de la même façon

Anonymisé

- Identification impossible en pratique, par quelque moyen que ce soit
- Irréversible : aucune table ne permet de revenir en arrière
- La donnée sort du RGPD
- Exemple : le nombre de réclamations par mois et par type, sans aucun client

Pseudonymisé

- Les noms remplacés par des étiquettes, la correspondance gardée à part
- Réversible avec la table de correspondance
- La donnée reste personnelle, le RGPD s'applique
- Exemple : le compte rendu où chaque candidat devient [Candidat A], [Candidat B]

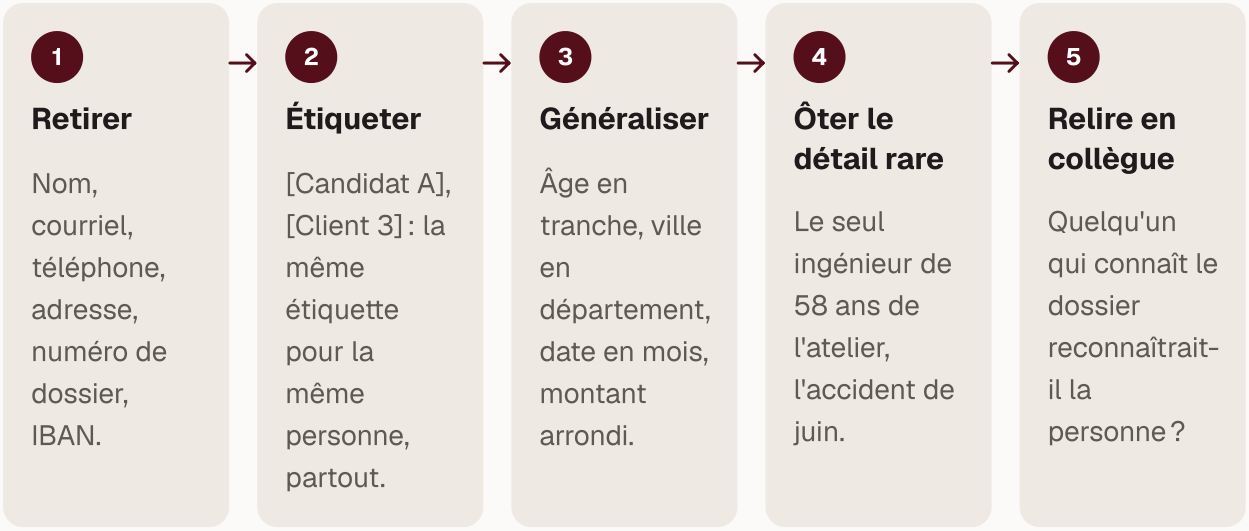
Définitions de la CNIL et de l'article 4, point 5, du RGPD. Avant un envoi à une IA, vous faites presque toujours une pseudonymisation.

Pour juger qu'un jeu de données est vraiment anonyme, la CNIL reprend les trois critères de l'avis 05/2014 des autorités européennes. L'**individualisation** : il ne doit plus être possible d'isoler une personne ; remplacer un nom par un numéro unique ne suffit donc pas. La **corrélation** : il ne doit plus être possible de relier deux ensembles de données concernant la même personne ; un tableau des primes et un tableau des absences qui partagent le même identifiant échouent à ce test. L'**inférence** : il ne doit plus être possible de déduire avec une quasi-certitude une information sur une personne ; « tous les techniciens de l'équipe de nuit ont eu une sanction » en dit long sur chacun d'eux. Les deux familles de techniques citées par la CNIL sont la randomisation (rendre les valeurs moins précises en gardant leur répartition) et la généralisation (élargir l'échelle : l'année au lieu de la date de naissance).

> **Demander à l'IA d'anonymiser, c'est déjà lui envoyer**
>
> Coller le texte brut dans un assistant pour qu'il remplace les noms, c'est transmettre ces noms à l'éditeur, avant toute protection. Deux voies seulement sont propres. La première : remplacer vous-même, sur votre poste, avec la fonction Rechercher et remplacer de Word ou une colonne d'identifiants dans Excel. La seconde : faire faire ce travail par l'**offre professionnelle de l'entreprise**, sous contrat de sous-traitance, entraînement exclu, et inscrite au registre, parce que cet outil peut déjà recevoir ces données. Jamais par un compte gratuit ou personnel.

La méthode en cinq gestes

Les cinq gestes avant d'envoyer un texte ou un fichier



Faits sur votre poste, avant l'envoi. La table de correspondance ne quitte jamais l'entreprise.

1. Retirer les identifiants directs : nom, prénom, courriel, téléphone, adresse, numéro de client, de dossier ou de contrat, IBAN, immatriculation, signature en bas de message.
2. Remplacer chaque personne par une étiquette stable, [Candidat A], [Client 3], [Salariée B], la même dans tout le texte et dans tous les envois du même dossier, et noter la correspondance dans un fichier à part, hors de l'IA.
3. Généraliser ce qui reste utile : l'âge en tranche (40 à 49 ans), la ville en département ou en zone (rive droite de Bordeaux), la date en mois, le montant arrondi à la centaine.
4. Retirer le détail rare qui trahit : le seul ingénieur de 58 ans de l'atelier, la cliente qui a appelé trois fois le jour de Noël, l'accident de la presse en juin.
5. Relire le résultat comme un collègue qui connaît le dossier : s'il reconnaît quelqu'un, recommencez au geste 3 ou 4.

Une ligne du dossier de recouvrement de Julien, avant et après

Avant	Après	Geste
Mme Hélène Roux, 12 allée des Pins, 33500 Libourne	[Client 1], Libournais	Retirer, étiqueter, généraliser
06 00 00 00 12, h.roux@exemple.fr	(supprimé)	Retirer
Facture n° 2026-0412 du 14 mars 2026, 1 846,20 € TTC	Facture de mars 2026, environ 1 850 € TTC	Généraliser
« A dit au téléphone qu'elle sortait de l'hôpital »	(supprimé)	Retirer : santé, inutile à la relance

Avant	Après	Geste
Cliente depuis 1998, seule à commander du sauternes en magnum	Cliente de longue date	Ôter le détail rare
Trois relances sans réponse, la dernière le 2 octobre	Trois relances sans réponse, la dernière début octobre	Garder, généraliser la date

Remplacer un nom partout dans un document Word

1. Travaillez sur une copie du document : Fichier, puis Enregistrer sous, avec un nom comme « compte-rendu-pseudonymise ». Les libellés peuvent varier selon la version de Word : repérez les emplacements décrits.
2. Dans l'onglet Accueil, groupe Modification, cliquez sur Remplacer (ou tapez Ctrl+H).
3. Dans la zone Rechercher, tapez le nom à remplacer, par exemple « Roux » ; dans la zone Remplacer par, tapez l'étiquette « [Client 1] ».
4. Ouvrez les options supplémentaires (bouton Autres ou Plus) et cochez l'option qui limite la recherche aux mots entiers, pour ne pas toucher « Rouxel ».
5. Cliquez sur Remplacer tout, notez le nombre de remplacements annoncé, puis recommencez avec le prénom, le courriel et le téléphone.
6. Notez « Roux = [Client 1] » dans votre table de correspondance, enregistrée dans un dossier à accès restreint, jamais dans le document envoyé.

Préparer un tableur, un document ou une photo

Un **tableur** se prépare en supprimant d'abord les colonnes dont la tâche n'a pas besoin, puis en remplaçant la colonne des noms par une colonne d'identifiants (la méthode suit). Un **document Word ou un PDF** porte plus que son texte : auteur et société dans les propriétés, commentaires, suivi des modifications, texte masqué. L'Inspecteur de document de Word les retire, sur une copie, car Microsoft prévient que les données supprimées ne peuvent pas toujours être restaurées ; il ne repère pas un texte écrit en blanc sur fond blanc. Une **photo** se recadre ou se floute avant l'envoi : visage, plaque d'immatriculation, badge, écran d'ordinateur en arrière-plan.

Inspecter un document Word avant de le joindre

1. Ouvrez la copie pseudonymisée du document, pas l'original. Les libellés peuvent varier selon la version : repérez les emplacements décrits.
2. Onglet Fichier, puis Info, puis Vérifier les problèmes, puis Inspecter le document.
3. Laissez cochés les commentaires et révisions, les propriétés du document et informations personnelles, le texte masqué, puis cliquez sur Inspecter.
4. Pour chaque catégorie trouvée, cliquez sur Supprimer tout, puis enregistrez.
5. L'Inspecteur de document n'existe pas dans toutes les versions de Word, notamment sur le web : supprimez alors les commentaires et acceptez les modifications à la main, depuis l'onglet Révision.

Remplacer une colonne de noms par des identifiants dans Excel TEXT

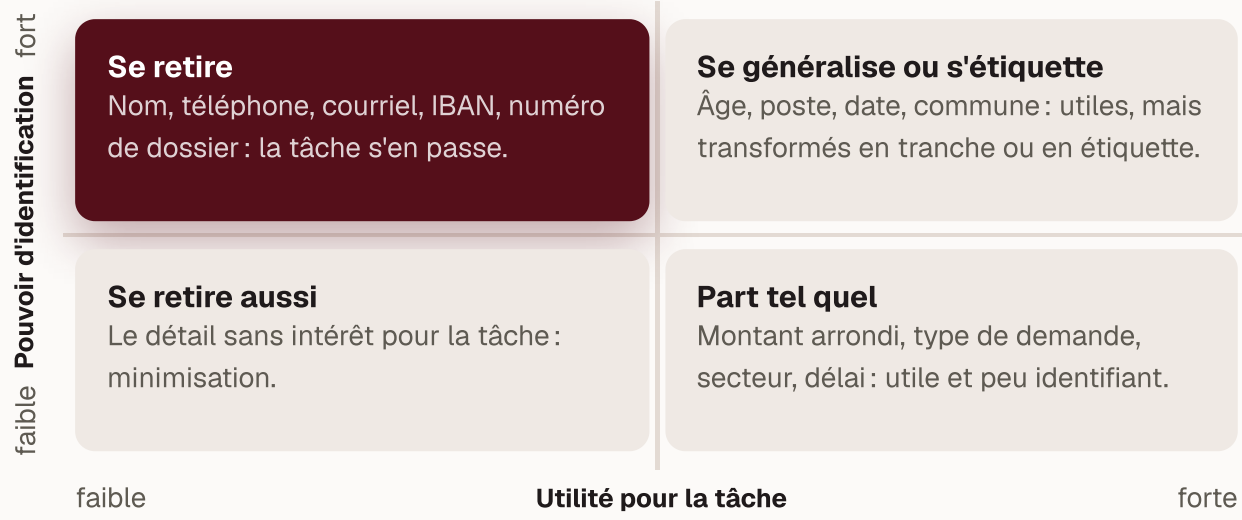
```
1. Onglet Correspondance : collez la colonne des noms en A (titre en A1).
   Onglet Données > Supprimer les doublons : il reste un nom par ligne.
2. En B2, l'identifiant de chaque nom, puis recopiez vers le bas :
   ="Client "&TEXTE(LIGNE()-1;"000")
   (donne Client 001, Client 002...)
3. Dans le tableau à envoyer, nouvelle colonne à côté des noms, en ligne 2 :
   =RECHERCHEX(A2;Correspondance!A:A;Correspondance!B:B;"à vérifier")
4. Copiez la nouvelle colonne, collez-la en valeurs (Collage spécial > Valeurs),
   puis supprimez la colonne des noms et toutes les colonnes inutiles.
5. Déplacez l'onglet Correspondance dans un classeur à part, rangé dans un
   dossier à accès restreint. Le classeur envoyé n'en garde aucune trace.
```

RECHERCHEX existe dans Excel pour Microsoft 365, Excel 2021 et 2024, selon l'aide de Microsoft relevée le 19/11/2026 ; pas dans Excel 2016 ni 2019, où RECHERCHEV la remplace. Une ligne « à vérifier » signale un nom mal orthographié.

Ce qui ne s'anonymise pas, et la limite des petites équipes

Certains contenus restent personnels quoi que vous fassiez au texte qui les accompagne : un enregistrement de voix, une photo de visage, un document manuscrit, une signature scannée. Ils ne partent pas dans une IA sans une raison solide, un outil professionnel et l'information des personnes. Et il faut le dire honnêtement : dans une PME de 15 personnes, presque tout est identifiable. « La comptable », « le nouveau commercial », « l'équipe du samedi » désignent des personnes. L'objectif réaliste n'est donc pas l'anonymat parfait, mais la combinaison de trois protections : pseudonymiser, n'envoyer que l'utile, et n'utiliser qu'un outil professionnel sous contrat, que la leçon « Choisir une offre d'IA selon l'entraînement, la conservation, le contrat et l'hébergement » apprend à choisir.

Ce qui part, ce qui se généralise, ce qui se retire



Chaque information se place selon ce qu'elle apporte à la tâche et ce qu'elle dit de la personne.

Pseudonymiser et vérifier avec l'IA de l'entreprise

Demande à recopier **Pseudonymiser un texte, uniquement dans l'outil professionnel de l'entreprise**

```
Tu aides un salarié d'une PME à préparer un texte avant son analyse.
Remplace dans le texte ci-dessous chaque personne par une étiquette stable ([Personne A], [Personne B]…) et chaque entreprise cliente par [Entreprise 1], [Entreprise 2]…, la même étiquette pour la même personne partout.
Supprime les courriels, téléphones, adresses, numéros de dossier et IBAN.
Remplace les dates précises par le mois et l'année, les âges par une tranche de dix ans, les montants par un arrondi à la centaine.
Supprime toute mention de santé, d'opinion, de religion, de mandat syndical ou de condamnation, en écrivant [mention retirée].
Rends deux parties : le texte transformé, puis la table de correspondance (étiquette = élément d'origine), que je copierai hors de cette conversation avant de la supprimer.
Texte : [collez le texte]
```

Ce que vous devez obtenir : Le texte transformé, avec ses étiquettes et ses mentions retirées, puis une table de cinq à quinze lignes. Vous copiez la table dans un fichier à accès restreint, vous effacez la conversation de l'historique, et vous relisez le texte vous-même avant tout usage.

Note : À ne faire que dans l'offre professionnelle de l'entreprise, sous contrat de sous-traitance et entraînement exclu. Avec un compte gratuit, remplacez à la main dans Word.

Demande à recopier **Vérifier qu'un texte pseudonymisé ne permet plus de reconnaître quelqu'un**

```
Ce texte a été pseudonymisé : les étiquettes entre crochets remplacent des personnes et des entreprises.
Contexte de lecture : il sera lu par [qui le lira : l'équipe de 14 personnes, un client, un prestataire].
Dis si une personne peut encore y être reconnue, seule ou par recoupement avec ce que ces lecteurs savent probablement.
Pour chaque passage en cause : la citation exacte, le critère en jeu (individualisation, corrélation ou inférence), une reformulation.
Si aucun passage ne pose problème, écris-le en une phrase.
Texte : [collez le texte pseudonymisé]
```

Ce que vous devez obtenir : Une liste courte : « la seule commerciale du secteur Médoc » (individualisation), « revenue de congé maternité en mars » (inférence, santé), chacun avec une reformulation. Vous tranchez : c'est vous qui savez qui lira le texte.

Où ranger la table de correspondance

Dans un fichier à part, dans un dossier réseau ou un espace partagé dont l'accès est limité aux personnes qui travaillent sur le dossier. Jamais dans le fichier envoyé, jamais collée dans une conversation, jamais en pièce jointe d'un courriel au prestataire. Datez-la et supprimez-la quand le dossier est clos : une table oubliée transforme n'importe quel fichier pseudonymisé en fichier nominatif.

Les erreurs fréquentes

L'erreur, et pourquoi elle coûte	La correction
Coller le texte brut dans un assistant gratuit pour qu'il « retire les noms ». Les noms, les coordonnées et les détails sensibles partent chez l'éditeur avant toute protection, dans un compte qui n'est lié à l'entreprise par aucun contrat.	Remplacez à la main dans Word ou dans Excel sur votre poste, ou utilisez l'offre professionnelle de l'entreprise, sous contrat de sous-traitance et entraînement exclu.
Garder la table de correspondance dans le fichier envoyé, dans un onglet caché, ou la coller dans la conversation. La table rend la pseudonymisation réversible pour quiconque la lit. Un onglet masqué part avec le classeur ; une table collée dans la conversation reste dans l'historique de l'éditeur.	Rangez la table dans un fichier distinct, en accès restreint, et supprimez-la à la clôture du dossier. Vérifiez qu'aucun onglet masqué ne reste dans le classeur envoyé.
Appeler « anonymisé » un fichier où les noms sont seulement remplacés par des numéros, puis relâcher les précautions. Avec une table, ou dans une petite équipe où les détails restants isolent une personne, le fichier reste personnel : le RGPD s'applique, l'outil doit être sous contrat, la conservation reste à régler.	Dites « pseudonymisé » tant qu'une table existe ou qu'une personne reste isolable ; réservez « anonymisé » aux agrégats qui passent les trois critères de la CNIL.
Soigner le texte et oublier ce que le fichier porte en plus. Auteur et société dans les propriétés, commentaires de marge, suivi des modifications, visage ou badge sur une photo : ces éléments partent avec le fichier et identifient aussi bien qu'un nom.	Passez l'Inspecteur de document sur une copie, acceptez les modifications, recadrez ou floutez les photos, et rouvrez le fichier final avant de le joindre.

Exercice : Préparer les verbatims d'une enquête avant de les faire analyser

Léa, cheffe de projet à l'agence de communication des Chartrons (14 personnes), doit faire analyser par l'assistant d'IA de l'agence les réponses libres d'une enquête de satisfaction menée pour un client, un réseau de six caves à vins de Gironde. Voici cinq verbatims, tels qu'ils ont été reçus (noms et coordonnées inventés). 1. « Paul Lafargue, paul.lafargue@exemple.fr : accueil parfait à la cave de Saint-Émilion, Margaux m'a très bien conseillé. » 2. « Très déçue par le livreur, qui m'a parlé sèchement devant mes enfants. Anne Dubreuil, 06 00 00 00 27. » 3. « En fauteuil roulant, je ne peux pas entrer dans la cave de Cadillac : la marche est trop haute. » 4. « Je suis client depuis 30 ans, j'étais le premier abonné à la box du mois. J.-M. Castaing. » 5. « Le caviste de Blaye, le grand barbu, ne connaît rien au bio. » Préparez ces verbatims pour l'analyse, construisez la table de correspondance et écrivez la demande d'analyse.

1. Relevez dans chaque verbatim les identifiants directs, les détails rares et les données sensibles.
2. Décidez pour chacun : retirer, étiqueter, généraliser.
3. Construisez la table de correspondance et dites où vous la rangez.

4. Réécrivez les cinq verbatims.
5. Écrivez la demande d'analyse et dites si le résultat est anonymisé ou pseudonymisé.

Le corrigé est dans le cahier d’exercices et sur la page de la leçon.

À retenir

- Anonymiser est irréversible et sort la donnée du RGPD ; pseudonymiser se défait avec la table de correspondance et laisse la donnée personnelle.
- Avant un envoi à une IA, vous faites presque toujours une pseudonymisation : utile, mais le RGPD continue de s'appliquer.
- Cinq gestes : retirer les identifiants, étiqueter de façon stable, généraliser, ôter le détail rare, relire en collègue.
- Demander à une IA d'anonymiser un texte brut, c'est déjà le lui envoyer : remplacez à la main, ou passez par l'offre professionnelle sous contrat.
- La table de correspondance vit à part, en accès restreint, et disparaît avec le dossier ; voix, visage et manuscrit restent personnels.

02

Choisir ses outils et tenir ses obligations

Choisir une offre dont le contrat et les réglages conviennent, puis inscrire l'usage au registre et prévenir les personnes concernées.

3 Choisir une offre d'IA selon l'entraînement, la conservation, le contrat et l'hébergement

4 Inscrire un usage de l'IA au registre et informer les personnes concernées

Leçon 3 | 32 min | Accès libre

Choisir une offre d'IA selon l'entraînement, la conservation, le contrat et l'hébergement

> Avant de confier des données de clients ou de salariés à une IA, posez cinq questions à l'offre : entraînement, conservation, contrat de sous-traitance, hébergement, transferts hors Union. Une offre grand public laisse ces choix à chaque salarié ; une offre professionnelle les fixe par contrat avec l'entreprise. Pour des données personnelles, seule la seconde convient.

Objectifs

- Poser les cinq questions de la grille à une offre d'IA et décider quoi faire d'une mauvaise réponse
- Distinguer une offre grand public d'une offre professionnelle par le contrat, le rôle de l'éditeur et les réglages
- Désactiver l'entraînement dans les outils grand public et obtenir le contrat de sous-traitance d'une offre professionnelle

Le cours

À l'agence de communication des Chartrons, Thomas, le directeur, prépare un appel d'offres avec Léa. Sur l'écran de Léa, il remarque l'historique d'un assistant d'IA : « Brief salon des vins, version 3 », « Retours client caves de Gironde ». Le compte est un compte gratuit, ouvert avec son adresse personnelle. Le lendemain, il apprend que deux autres salariés font de même. Personne n'a mal agi par intention ; mais à la question du cours, « qu'est-ce qui part, chez qui, pour quoi faire, et qui le sait ? », la réponse est inquiétante : les briefs des clients partent chez un éditeur avec lequel l'agence n'a aucun contrat, et personne à l'agence ne le savait.

Grand public ou professionnel, la différence est dans le contrat

Avec une **offre grand public**, gratuite ou payée par un abonnement individuel, le salarié est client à titre personnel. L'éditeur décide de ce qu'il fait des conversations, comme responsable de traitement, dans les limites de sa politique de confidentialité ; les réglages, dont l'entraînement des modèles, sont laissés à chaque utilisateur. Avec une **offre professionnelle**, l'entreprise signe ou accepte un contrat : l'éditeur agit comme **sous-traitant** au sens de l'article 28 du RGPD, sur ses instructions documentées, avec des obligations de sécurité, de confidentialité, d'aide et de suppression des données en fin de contrat. L'entraînement y est exclu par défaut chez la plupart des éditeurs, et une console d'administration règle les comptes et la conservation pour tous. La Commission nationale de l'informatique et des libertés (CNIL) recommande, dans ses questions-réponses du 18/07/2024, d'éviter les comptes créés avec des

adresses personnelles et de ne jamais partager de données personnelles ou confidentielles avec un service grand public.

Une offre grand public, une offre professionnelle

Grand public (gratuit ou abonnement individuel)

- Le salarié est client à titre personnel
- L'éditeur décide de l'usage des conversations, comme responsable de traitement
- Entraînement souvent activé par défaut, réglage laissé à chacun
- Aucun contrat de sous-traitance avec l'entreprise

Professionnelle (contrat avec l'entreprise)

- L'entreprise est cliente et responsable du traitement
- L'éditeur agit comme sous-traitant, sur instruction (article 28)
- Entraînement exclu par défaut chez la plupart des éditeurs
- Console d'administration : comptes, conservation, réglages pour tous

La différence tient au contrat et au rôle de l'éditeur, pas au prix de l'abonnement.

Le compte gratuit personnel, première fuite de données des PME

Notre opinion, sans détour : un compte personnel gratuit n'a rien à faire dans un dossier de client ou de salarié. Il n'existe aucun contrat entre l'entreprise et l'éditeur, les réglages dépendent de chacun, l'historique part avec le salarié le jour où il quitte l'entreprise, et personne ne peut répondre à un client qui demande où sont passées ses données. Un abonnement individuel payant ne change rien à ce constat : c'est toujours une offre grand public.

Les cinq questions à poser à toute offre

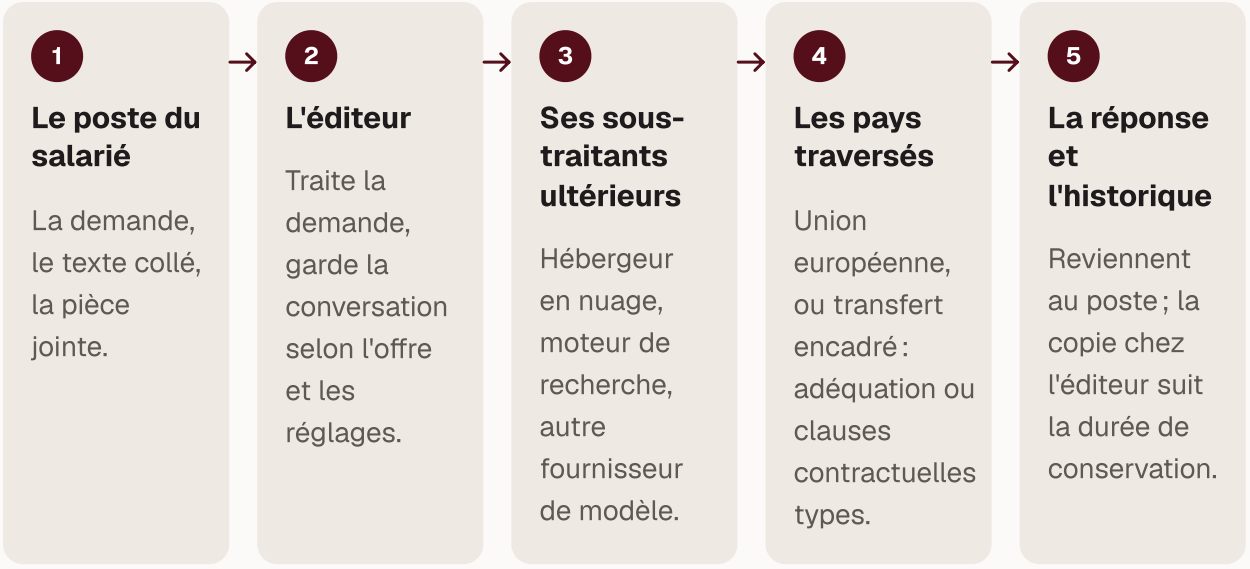
La grille, et la conduite à tenir quand la réponse est mauvaise

Question	Bonne réponse	Si la réponse est mauvaise
1. Mes conversations entraînent-elles les modèles, et comment m'y opposer ?	Exclu par défaut, ou coupé par l'administrateur pour tous	Outil réservé aux textes sans donnée personnelle, ou réglage imposé à tous les comptes
2. Combien de temps sont-elles conservées, y compris après suppression ?	Durée connue, réglable par l'administrateur, suppression effective sous un délai annoncé	Purge régulière par les utilisateurs, et durée inscrite au registre telle qu'elle est
3. Un contrat de sous-traitance (DPA, article 28) existe-t-il, et qui le signe ?	DPA intégré aux conditions professionnelles ou signé par l'entreprise	Aucune donnée personnelle tant qu'il n'est pas obtenu et rangé

Question	Bonne réponse	Si la réponse est mauvaise
4. Où sont hébergées les données, et une résidence en Europe est-elle possible ?	Pays nommé ; option européenne quand elle existe	Demander la liste des sous-traitants ultérieurs et leurs pays
5. Les données sortent-elles de l'Union, et sur quel fondement ?	Décision d'adéquation (Data Privacy Framework) ou clauses contractuelles types (articles 44 à 49)	Pas de données personnelles sans fondement de transfert écrit

Les transferts méritent une phrase de plus. Pour les États-Unis, la Commission européenne a adopté le 10/07/2023 une décision d'adéquation, le Data Privacy Framework. Le Tribunal de l'Union l'a jugée valide le 3/9/2025 (affaire T-553/23) ; un pourvoi est pendant devant la Cour de justice (affaire C-703/25 P) : elle est donc **valide à ce jour, et contestée**. Un transfert vers une entreprise américaine certifiée n'exige pas d'autre outil ; vers une entreprise non certifiée, il suppose des clauses contractuelles types, le plus souvent intégrées au DPA de l'éditeur. Un hébergement en Europe ne règle pas tout : l'éditeur peut faire traiter une partie des demandes ailleurs, par ses sous-traitants ultérieurs, d'où la question 4.

Le trajet d'une demande envoyée à une IA



À chaque étape, une question : qui traite, sous quel contrat, dans quel pays.

Cinq éditeurs relevés le 19/11/2026

Les conditions de cinq éditeurs, relevé du 19/11/2026 sur leurs pages officielles

Éditeur et offre	Entraînement	Réglage ou contrôle	Conservation	Contrat	Hébergement
OpenAI, ChatGPT Free, Plus, Pro	Activé par défaut	Paramètres › Commandes des données › « Améliorer le modèle pour tout le monde »	Jusqu'à suppression ; supprimé sous 30 jours, sauf obligation de sécurité ou légale ; discussion temporaire gardée jusqu'à 30 jours	Aucun avec l'entreprise	Non relevé
OpenAI, ChatGPT Business, Enterprise, Edu, API	Exclu par défaut	Console d'administration	Réglée par l'administrateur en Enterprise	DPA par formulaire en ligne	Résidence européenne pour Enterprise et Edu ; région Europe de l'API pour les organisations éligibles
Anthropic, Claude Free, Pro, Max	Choix demandé à chaque utilisateur depuis le 8/10/2025	Paramètres › Confidentialité › « Help improve our AI models »	Supprimé sous 30 jours ; jusqu'à 5 ans si l'entraînement est accepté	Aucun avec l'entreprise	Non relevé
Anthropic, Claude Team, Enterprise, API	Exclu par défaut, sauf avis envoyés par les membres	Le propriétaire peut couper les avis	Selon le contrat	DPA intégré aux conditions commerciales, clauses contractuelles types comprises	Stockage aux États-Unis ; traitement possible dans plusieurs régions
Google, application Gemini	Activé avec l'historique	Historique Gemini (myactivity.google.com/product/gemini)	18 mois par défaut ; environ 2 mois historique coupé ; jusqu'à 3 ans si relu par un réviseur humain	Aucun avec l'entreprise	Non relevé
Google, Gemini dans Workspace	Pas sans permission du client ; pas de relecture humaine	Console d'administration	3, 18 ou 36 mois, 18 par défaut	Cloud Data Processing Addendum	Non relevé ; Google adhère au Data Privacy Framework
Microsoft, Copilot grand public	Activé par défaut, sauf exceptions (comptes professionnels, mineurs, certains pays)	Rubrique Confidentialité du profil	18 mois par défaut	Aucun avec l'entreprise	Non relevé

Éditeur et offre	Entraînement	Réglage ou contrôle	Conservation	Contrat	Hébergement
Microsoft 365 Copilot, Copilot Chat (compte professionnel)	Pas d'entraînement des modèles de base	Purview, administration Microsoft 365	Selon les règles de conservation de l'entreprise	Data Protection Addendum, Product Terms	EU Data Boundary, qui ne couvre ni la recherche web ni les modèles d'Anthropic proposés dans Copilot
Mistral, Vibe (anciennement Le Chat) Free, Pro	Activé par défaut	Sur mobile : Settings › Data & Account Controls › décocher « Enable data sharing »	Non relevé	Aucun avec l'entreprise	Espace économique européen par défaut
Mistral, Vibe Teams, Enterprise, API Studio	Activé par défaut en Teams, désactivé en Enterprise	Console admin.mistral.ai › Vibe › Privacy	API : 30 jours glissants pour la surveillance des abus	DPA intégré au contrat	Espace économique européen par défaut

Professionnel ne veut pas toujours dire sans entraînement

Trois pièges relevés le 19/11/2026. Chez Mistral, l'offre Vibe Teams laisse l'entraînement activé tant que l'administrateur ne l'a pas coupé pour l'organisation. Chez Anthropic, les avis envoyés par les membres d'une équipe (les pouces sous une réponse) peuvent servir, sauf si le propriétaire les coupe. Chez Microsoft, la frontière de données européenne ne couvre ni la recherche web ni les modèles d'Anthropic proposés dans Copilot. Vérifiez la page officielle le jour où vous choisissez : ces conditions changent plusieurs fois par an.

Couper l'entraînement d'un compte grand public

Dans ChatGPT, sur le web

1. Les libellés peuvent varier selon la version et la langue de l'interface : repérez les emplacements décrits. Relevé du 19/11/2026.
2. Ouvrez le menu de votre compte, en bas à gauche, puis Paramètres (Settings).
3. Ouvrez la rubrique Commandes des données (Data controls).
4. Choisissez « Améliorer le modèle pour tout le monde » (Improve the model for everyone), désactivez-le, puis validez. Le réglage vaut pour tout le compte, web et mobile.
5. Le mode vocal a son propre réglage de partage des données, dans la même rubrique : coupez-le aussi.

Dans Claude, sur le web ou l'application de bureau

1. Les libellés peuvent varier selon la version : repérez les emplacements décrits. Relevé du 19/11/2026.
2. Cliquez sur votre nom dans le menu, puis sur Paramètres (Settings).
3. Ouvrez Confidentialité (Privacy).
4. Sous « Help improve our AI models » (aider à améliorer nos modèles), désactivez l'interrupteur. Les nouvelles conversations ne serviront plus à entraîner les modèles ; ce qui est déjà entré dans un entraînement en cours n'en sort pas.

Dans l'application Gemini et dans Vibe

1. Les libellés peuvent varier selon la version : repérez les emplacements décrits. Relevé du 19/11/2026.
2. Gemini : ouvrez myactivity.google.com/product/gemini, connecté au compte concerné, et désactivez l'historique Gemini. Les conversations futures ne serviront plus à l'entraînement, mais restent gardées environ 2 mois.
3. Gemini : sur la même page, réglez la suppression automatique sur 3 mois pour l'historique déjà enregistré.
4. Vibe sur mobile : ouvrez Settings, rubrique Account, puis Data & Account Controls, et décochez « Enable data sharing ».
5. Vibe pour une équipe : l'administrateur ouvre admin.mistral.ai, choisit Vibe sous Manage, puis Privacy, et coupe l'interrupteur qui autorise l'entraînement. Le réglage de l'API Studio est distinct, dans le menu Privacy de la même console.

Couper l'entraînement réduit un risque, il ne transforme pas un compte grand public en outil professionnel. Il n'y a toujours aucun contrat, les conversations restent conservées (jusqu'à 3 ans chez Google pour celles qu'un réviseur humain a lues, même après suppression), et le salarié peut réactiver le réglage demain. Ces comptes, réglés, servent aux textes sans aucune donnée personnelle : reformuler une offre publique, préparer une trame, traduire une plaquette.

Obtenir les documents et décider

Demande à recopier **Faire lire la page de confidentialité d'un éditeur selon la grille**

```
Tu aides une PME de [effectif] personnes à choisir un outil d'IA.
Voici le texte copié de la page officielle de confidentialité et des conditions de
l'offre [nom de l'offre] de [éditeur], relevé le [date] : [collez le texte].
Réponds aux cinq questions suivantes, en citant pour chacune la phrase exacte du texte
qui fonde ta réponse :
1. Les conversations servent-elles à entraîner les modèles, et comment s'y opposer ?
2. Combien de temps sont-elles conservées, y compris après suppression ?
3. Un contrat de sous-traitance (DPA) existe-t-il, et comment est-il accepté ou signé ?
4. Où les données sont-elles hébergées, et une résidence en Europe est-elle possible ?
5. Les données sortent-elles de l'Union européenne, et sur quel fondement ?
```

```
Si le texte ne répond pas, écris « non trouvé » : ne complète jamais avec ce que tu crois savoir de cet éditeur.
```

Ce que vous devez obtenir : Cinq réponses courtes, chacune suivie d'une citation, et plusieurs « non trouvé » (souvent l'hébergement et les transferts, qui figurent dans d'autres pages). Chaque « non trouvé » devient une question à l'éditeur ou au revendeur.

Note : Collez le texte de la page officielle, pas un article de blog. L'IA ne doit pas répondre de mémoire : ses connaissances sur un éditeur peuvent dater de plusieurs mois.

Demande à recopier **Écrire au revendeur ou à l'éditeur pour obtenir le contrat**

```
Rédige un courriel court et précis à [revendeur ou éditeur], de la part de [prénom, fonction] d'une PME de [effectif] personnes, cliente ou future cliente de l'offre [nom de l'offre].
Nous demandons, avant de déployer l'outil auprès de [nombre] utilisateurs :
1. le contrat de sous-traitance (DPA) applicable, conforme à l'article 28 du RGPD, et la façon de l'accepter ou de le signer ;
2. la liste à jour des sous-traitants ultérieurs, avec leur pays ;
3. le pays d'hébergement et de traitement des données, et l'existence d'une option de résidence dans l'Union européenne ;
4. le fondement des transferts hors de l'Union, le cas échéant ;
5. la confirmation que nos conversations ne servent pas à entraîner les modèles, et la durée de conservation applicable.
Ton cordial, 15 lignes au plus, avec une date de réponse souhaitée sous 10 jours ouvrés.
```

Ce que vous devez obtenir : Un courriel de cinq demandes numérotées, avec la date de réponse souhaitée. Les réponses reçues se rangent avec le DPA, en PDF daté, dans le dossier de l'outil, et nourrissent la ligne du registre.

Cet outil peut-il recevoir des données de clients

1 **Le compte appartient-il à l'entreprise, sous une offre professionnelle ?**

Non

Fermez l'usage professionnel du compte personnel ; ouvrez un compte d'entreprise.

2 **Un contrat de sous-traitance (DPA) est-il accepté ou signé, et rangé ?**

Non Obtenez-le avant tout envoi : sans contrat, pas de données personnelles.

3 **L'entraînement sur vos conversations est-il exclu, par défaut ou par un réglage de l'administrateur ?**

Non Faites-le couper dans la console d'administration, pour tous les comptes.

4 **Savez-vous où les données sont hébergées et sur quel fondement elles sortent de l'Union ?**

Non Demandez la liste des sous-traitants ultérieurs et les garanties de transfert.

Oui à tout **Inscrivez l'outil au registre et notez la date du relevé des conditions.**

Un « non » : l'outil reste réservé aux textes sans aucune donnée personnelle.

La règle du cours, à appliquer telle quelle

Pour des données de clients ou de salariés : une offre professionnelle sous contrat, l'entraînement exclu, et l'outil inscrit au registre avec la date du relevé des conditions. Les offres gratuites, réglées, pour des textes sans aucune donnée personnelle. La fiche « La fiche d'un usage de l'IA » (fiche-usage-ia.docx) garde ces réponses sur une page par usage ; la leçon « Inscrire un usage de l'IA au registre et informer les personnes concernées » en fait la ligne du registre.

Les erreurs fréquentes

L'erreur, et pourquoi elle coûte	La correction
Prendre un abonnement individuel payant pour une offre professionnelle. Le prix ne crée pas de contrat : l'abonnement lie le salarié à l'éditeur, pas l'entreprise. Il n'y a ni DPA, ni console d'administration, ni réglage imposé à tous.	Souscrivez l'offre d'équipe ou d'entreprise au nom de la société, avec les adresses professionnelles, et rangez le DPA.
Couper l'entraînement d'un compte gratuit et le considérer comme apte aux données de clients. Le réglage ne crée ni contrat ni sous-traitance, la conservation continue (jusqu'à 3 ans chez Google pour une conversation relue), et le salarié peut le réactiver.	Gardez ces comptes, réglés, pour les textes sans aucune donnée personnelle, et passez les dossiers de clients sur l'offre professionnelle.
Supposer qu'une offre « équipe » exclut toujours l'entraînement. Au 19/11/2026, Vibe Teams l'active par défaut, et chez Anthropic les avis envoyés par les membres d'une équipe peuvent servir. Le défaut varie d'un éditeur à l'autre.	Ouvrez la console d'administration le jour de la souscription, coupez l'entraînement et les avis, et vérifiez sur un compte de test.
Croire qu'un hébergement en Europe empêche tout transfert. Les sous-traitants ultérieurs, la recherche web ou un modèle tiers peuvent traiter les données ailleurs : la frontière européenne de Microsoft exclut la recherche web et les modèles d'Anthropic, et Anthropic stocke les données aux États-Unis.	Demandez la liste des sous-traitants ultérieurs et leur pays, et notez dans le registre chaque transfert avec son fondement.

Exercice : Choisir l'offre du cabinet de recrutement

Karim, gérant du cabinet de recrutement et de conseil RH de Mérignac (9 personnes), veut équiper ses quatre chargés de recrutement d'un assistant d'IA pour rédiger des annonces, résumer des notes d'entretien pseudonymisées et préparer des synthèses pour les clients. Sophie utilise aujourd'hui un abonnement individuel payant, souscrit à son nom. Karim hésite entre trois offres d'équipe : ChatGPT Business, Claude Team et Vibe Teams. Appliquez la grille aux trois offres avec le tableau du relevé du 19/11/2026, dites ce qui manque, décidez, et listez ce qu'il faut faire avant le premier envoi.

1. Remplissez la grille des cinq questions pour chacune des trois offres, en écrivant « non relevé » quand le tableau ne dit rien.
2. Repérez, pour chaque offre, le réglage à faire ou la question à poser.
3. Dites ce que devient l'abonnement individuel de Sophie.
4. Décidez et justifiez en trois phrases.
5. Listez les gestes à faire avant le premier envoi de notes d'entretien.

Le corrigé est dans le cahier d'exercices et sur la page de la leçon.

À retenir

- La différence entre grand public et professionnel tient au contrat : avec un DPA, l'éditeur devient le sous-traitant de l'entreprise (article 28) ; un abonnement individuel payant reste grand public.
- Cinq questions à toute offre : entraînement, conservation, contrat de sous-traitance, hébergement, transferts hors Union, avec la date du relevé.
- Couper l'entraînement d'un compte gratuit réduit un risque, mais ce compte reste réservé aux textes sans donnée personnelle.
- Une offre professionnelle se vérifie aussi : entraînement actif par défaut en Vibe Teams, avis des membres chez Claude Team, recherche web hors frontière européenne chez Microsoft.
- Le Data Privacy Framework fonde les transferts vers les entreprises américaines certifiées : valide à ce jour, contesté devant la Cour de justice.

Leçon 4 | 32 min | Accès libre

Inscrire un usage de l'IA au registre et informer les personnes concernées

Un usage de l'IA modifie souvent un traitement existant, le recrutement ou la gestion des clients : sa ligne du registre s'enrichit d'un sous-traitant, d'un pays, d'une durée et d'une mesure. Vous vérifiez s'il faut une analyse d'impact, puis vous complétez la mention d'information des personnes concernées, candidats, clients et salariés compris.

Objectifs

- Rédiger ou compléter la ligne du registre (article 30 du RGPD) pour un usage de l'IA
- Décider s'il faut une analyse d'impact (article 35) à partir des neuf critères repris par la CNIL
- Compléter la mention d'information (articles 13 et 14) d'une offre d'emploi, d'un formulaire ou d'une politique de confidentialité

Le cours

Au cabinet de recrutement de Mérignac, Karim, le gérant, a équipé l'équipe d'une offre professionnelle d'IA pour préqualifier les candidatures : l'assistant résume les CV pseudonymisés et les rapproche de la fiche de poste, puis Sophie décide. Trois semaines plus tard, un candidat écrit : « Une intelligence artificielle a-t-elle lu mon CV ? Qui l'a vu, et pour combien de temps ? » Karim cherche la réponse dans son registre : l'outil n'y figure pas, et l'annonce n'en disait rien. La dernière partie de la question du cours, « qui le sait ? », se règle ici, en deux documents : le registre, pour l'entreprise et la CNIL, et la mention d'information, pour les personnes.

Le registre, même sous 250 salariés

L'article 30 du RGPD impose au responsable du traitement de tenir un registre des activités de traitement. Pour chaque traitement, il indique les finalités, les catégories de personnes concernées et de données, les destinataires, les transferts hors de l'Union, les délais d'effacement et une description générale des mesures de sécurité. Les organismes de moins de 250 salariés en sont dispensés, **sauf** pour les traitements non occasionnels, ceux qui présentent un risque pour les droits et libertés, et ceux qui portent sur des données sensibles ou des infractions. La Commission nationale de l'informatique et des libertés (CNIL) donne les exemples : la gestion de la paie, des clients, des prospects et des fournisseurs n'est pas occasionnelle. En pratique, toute PME qui paie des salariés ou suit des clients tient un registre ; la CNIL ajoute qu'en cas de doute, mieux vaut inscrire le traitement.

> **Le modèle simplifié de la CNIL**
>
> La CNIL met à disposition un modèle de registre simplifié, au format tableur, pensé pour les TPE et PME : registre-traitement-simplifie.ods, sur sa page « Le registre des activités de traitement ». Il s'ouvre dans Excel ou LibreOffice. Une ligne par traitement, une colonne par rubrique : c'est là que vos usages de l'IA trouvent leur place.

Un usage de l'IA enrichit souvent une ligne existante

Utiliser une IA ne crée pas forcément un nouveau traitement. Quand Sophie fait résumer des CV, la finalité reste la même, recruter ; le traitement « gestion des recrutements » existait avant l'outil. Sa ligne s'enrichit de quatre éléments : un **destinataire**, l'éditeur de l'offre d'IA, comme sous-traitant, avec la date de son contrat ; un **pays** et le fondement du transfert si les données sortent de l'Union ; une **durée**, celle des conversations chez l'éditeur ; des **mesures**, pseudonymisation, entraînement exclu, comptes nominatifs. Un nouveau traitement naît quand l'IA sert une finalité qui n'existait pas : analyser le ton des avis clients pour noter les vendeurs, par exemple. Rangez le registre par finalité, jamais par outil : une ligne « ChatGPT » ne dit à personne ce qui est fait des données.

La ligne du registre, rubrique par rubrique

Traitement et responsable
Le nom du traitement (verbe et objet), l'entreprise, la personne qui en répond.

Finalité
Pourquoi les données sont traitées, et ce que l'IA y fait : résumer, trier, rédiger.

Personnes et données
Catégories de personnes (candidats, clients) et de données ; ce qui part vers l'IA, ce qui n'y part pas.

Destinataires et sous-traitants
Services internes, et l'éditeur de l'offre d'IA comme sous-traitant, avec son contrat.

Transferts hors Union
Le pays et le fondement : décision d'adéquation ou clauses contractuelles types.

Durées et sécurité
La durée chez vous et chez l'éditeur ; pseudonymisation, entraînement exclu, comptes nominatifs.

Les rubriques de l'article 30 du RGPD. En gras dans votre tableur : ce que l'usage de l'IA ajoute à une ligne existante.

La ligne du cabinet RH, préqualification des candidatures avec un assistant d'IA

Rubrique	Contenu
Traitement et responsable	Gestion des recrutements pour le compte des clients ; responsable : le cabinet, représenté par Karim, gérant
Finalité	Recevoir, préqualifier et présenter des candidatures ; l'assistant d'IA résume les CV pseudonymisés et les rapproche de la fiche de poste ; une chargée de recrutement lit chaque dossier et décide
Personnes concernées	Candidats
Données	Identité, coordonnées, parcours, diplômes, notes d'entretien, prétentions ; vers l'IA : parcours et compétences sous étiquette [Candidat A], sans identité, âge ni donnée sensible

Rubrique	Contenu
Destinataires	Chargés de recrutement du cabinet ; client destinataire de la présélection ; éditeur de l'offre d'IA, sous-traitant (DPA accepté le [date], rangé dans le dossier de l'outil)
Transferts hors Union	Selon l'offre retenue : pays et fondement relevés le [date] (décision d'adéquation ou clauses contractuelles types)
Durées de conservation	Dossier de candidature selon la durée fixée par le cabinet ; conversations chez l'éditeur selon le réglage de l'administrateur, purge mensuelle
Mesures de sécurité	Offre professionnelle, entraînement exclu, comptes nominatifs, pseudonymisation avant envoi, table de correspondance en accès restreint, charte d'usage
Analyse d'impact	Présumée (évaluation de personnes et usage innovant) : menée avec le conseil du cabinet le [date]

Demande à recopier **Faire rédiger la ligne du registre à partir d'une description sans donnée personnelle**

```
Tu aides le référent RGPD d'une PME de [effectif] personnes, secteur [secteur].
Voici la description d'un usage de l'IA, sans aucune donnée personnelle réelle :
[traitement concerné, ce que fait l'IA, ce qui lui est envoyé et ce qui ne l'est pas,
offre utilisée et date de son contrat, réglages, qui relit].
Rédige la ligne de notre registre des activités de traitement selon l'article 30 du
RGPD, en neuf rubriques : traitement et responsable, finalité, personnes concernées,
données (en distinguant ce qui part vers l'IA), destinataires dont le sous-traitant
d'IA, transferts hors Union et fondement, durées de conservation (chez nous et chez
l'éditeur), mesures de sécurité, analyse d'impact (critères remplis parmi les neuf de
la CNIL, avec une phrase de justification chacun).
Écris « à compléter » pour toute information absente de la description : ne suppose
rien.
```

Ce que vous devez obtenir : Un tableau de neuf rubriques, avec plusieurs « à compléter », le plus souvent les transferts et la durée de conservation chez l'éditeur. Ces cases se remplissent avec la fiche d'usage et la page officielle de l'éditeur, jamais avec la seule réponse de l'IA.

Faut-il une analyse d'impact

L'article 35 du RGPD impose une analyse d'impact (AIPD) avant un traitement susceptible d'engendrer un risque élevé, notamment avec de nouvelles technologies ; elle est obligatoire pour le profilage à effets significatifs, les données sensibles à grande échelle et la surveillance systématique d'un lieu public à grande échelle. La CNIL reprend les neuf critères des lignes directrices européennes : évaluation ou notation, décision automatique à effet juridique ou similaire, surveillance systématique, données sensibles ou très personnelles, grande échelle, croisement de données, personnes vulnérables, usage innovant, exclusion du bénéfice d'un droit ou d'un contrat. Un traitement qui en remplit **deux** est présumé soumis à l'analyse d'impact. Pour l'IA, la CNIL précise que l'usage n'est pas systématiquement innovant, mais elle cite l'IA générative comme exemple d'usage innovant. Préqualifier des candidatures avec un assistant d'IA coche donc deux critères : l'évaluation et l'usage innovant.

Faut-il une analyse d'impact

1 **Le traitement évite-t-il d'évaluer ou de noter des personnes (profilage, tri, score) ?**

Non — Premier critère rempli : regardez les suivants avec attention.

2 **Évite-t-il toute décision automatique produisant un effet juridique ou similaire ?**

Non — Critère rempli, et l'article 22 du RGPD s'applique : une personne décide.

3 **Évite-t-il les données sensibles, la surveillance systématique, les personnes vulnérables et le croisement de fichiers ?**

Non — Critère rempli : notez lequel dans la fiche d'usage.

4 **Reste-t-il sous deux critères en comptant l'usage innovant, la grande échelle et l'exclusion d'un droit ?**

Non

Analyse d'impact présumée : associez votre DPO ou votre conseil avant la mise en service.

Oui à tout — **Pas d'analyse d'impact présumée : notez le décompte et sa date dans la fiche d'usage.**

Les neuf critères des lignes directrices européennes, repris par la CNIL. Deux critères remplis : l'analyse d'impact est présumée obligatoire.

L'analyse d'impact du RGPD n'est pas l'évaluation de l'AI Act

L'article 27 de l'AI Act, le règlement européen sur l'intelligence artificielle, prévoit une évaluation de l'impact sur les droits fondamentaux pour certains déployeurs de systèmes à haut risque : les organismes de droit public, les entités privées qui fournissent des services publics, et les utilisateurs des systèmes de l'annexe III, point 5, b et c (crédit et certaines assurances). Une PME privée qui utilise un outil d'aide au recrutement n'est pas visée par cet article. L'analyse d'impact du RGPD, elle, reste due dès que les critères sont remplis.

Informer les personnes concernées

Les articles 13 et 14 du RGPD disent ce que les personnes doivent savoir. Quand les données sont collectées auprès d'elles (un formulaire, une candidature envoyée par le candidat), l'information se donne **au moment de la collecte** (article 13). Quand elles viennent d'ailleurs (un CV transmis par un job board ou par un salarié qui coopte), elle se donne dans un délai raisonnable d'**un mois au plus**, ou au plus tard lors de la première communication avec la personne (article 14). Le contenu : identité du responsable et contact du DPO s'il y en a un, finalités et base juridique, intérêts légitimes le cas échéant, destinataires ou catégories de destinataires, transferts hors Union et garanties, durée de conservation, droits (accès, rectification, effacement, limitation, opposition, portabilité), droit de réclamation auprès de la CNIL, et l'existence d'une décision automatisée avec la logique sous-jacente.

- Offre d'emploi : « les candidatures sont préqualifiées avec l'aide d'un outil d'IA, puis lues par une chargée de recrutement qui décide » ; l'éditeur parmi les catégories de destinataires (prestataire d'outil d'IA) ; le pays s'il est hors Union ; la durée de conservation.
- Formulaire de contact : « votre demande est classée automatiquement, puis traitée par notre équipe » ; le lien vers la politique de confidentialité mise à jour.
- Politique de confidentialité : une ligne par traitement concerné, l'outil d'IA dans la liste des sous-traitants par catégorie, les transferts et leur fondement, et l'absence de décision fondée exclusivement sur un traitement automatisé, si c'est le cas.

Les salariés et les candidats ont aussi un texte à eux dans le Code du travail : aucune information les concernant personnellement ne peut être collectée par un dispositif qui n'a pas été porté préalablement à leur connaissance (article L1221-9 pour les candidats, article L1222-4 pour les salariés). Dans les entreprises d'au moins 50 salariés, le comité social et économique est informé et consulté sur l'introduction de nouvelles technologies (article L2312-8). Savoir si un outil d'IA précis en relève dépend de son effet sur le travail : la question se tranche avec votre juriste, avant le déploiement, pas après.

Demande à recopier **Faire réécrire la mention d'information d'une offre d'emploi**

```
Tu aides une PME de recrutement de [effectif] personnes à mettre à jour la mention
d'information placée sous ses offres d'emploi.
Voici la mention actuelle : [collez la mention].
Voici ce qui change : les candidatures sont préqualifiées avec l'aide d'un outil d'IA
de [offre professionnelle], sous-traitant, qui reçoit le parcours et les compétences
sans l'identité ; une chargée de recrutement lit chaque dossier et prend toute décision
; données hébergées [pays, fondement du transfert le cas échéant] ; conservation
[durée].
Réécris la mention en langage clair, 10 lignes au plus, en reprenant les informations
de l'article 13 du RGPD : responsable, finalité et base juridique, destinataires dont
le prestataire d'outil d'IA, transfert, durée, droits et adresse pour les exercer,
réclamation auprès de la CNIL. Dis explicitement qu'aucune décision n'est prise par
l'outil seul.
N'invente aucune information : laisse les [crochets] que je dois remplir.
```

Ce que vous devez obtenir : Une mention de huit à dix lignes, en phrases courtes, qui nomme l'aide de l'outil d'IA et la décision humaine, avec des [crochets] pour l'adresse de contact et la durée. Vous la relisez avec la ligne du registre : les deux doivent dire la même chose.

De l'idée d'usage à la mise en service

Semaine 1 — La fiche d'usage

Ce qui part, chez qui, pour quoi faire.

Semaine 1 — Le contrat

DPA de l'offre professionnelle rangé, entraînement exclu.

Semaine 2 — Le registre

Ligne complétée, analyse d'impact décidée.

Semaine 2 — L'information

Mentions mises à jour, salariés et CSE informés.

Semaine 3 — La formation et la mise en service

Utilisateurs formés, date notée, première relecture fixée.

Un calendrier type pour une PME, à adapter. Rien ne part vers l'IA avant la semaine 3.

Une fiche, trois usages

La fiche « La fiche d'un usage de l'IA » (fiche-usage-ia.docx) se remplit une fois par usage : elle devient la ligne du registre, une pièce de la charte d'usage et la preuve des mesures prises. Datez chaque case qui dépend de l'éditeur : ses conditions changent, et la relecture se fait au moins une fois par an, ou à chaque changement d'offre.

Les erreurs fréquentes

L'erreur, et pourquoi elle coûte	La correction
Créer au registre une ligne au nom de l'outil (« ChatGPT », « Copilot ») au lieu de compléter la ligne du traitement concerné. Le registre décrit des finalités. Une ligne par outil mélange recrutement, prospects et rédaction, et ne permet pas de répondre à une personne qui demande ce que devient sa candidature.	Complétez la ligne de chaque traitement où l'outil intervient : le sous-traitant, le pays, la durée et les mesures ; gardez la liste des outils dans la fiche d'usage.
Oublier la durée de conservation chez l'éditeur et les transferts. Les conversations et les fichiers restent chez l'éditeur selon l'offre et les réglages, parfois dans un autre pays. Une ligne qui ne cite que la durée interne est incomplète au regard de l'article 30.	Relevez la durée et le pays sur la page officielle de l'éditeur, notez-les avec la date du relevé, et réglez la conservation dans la console quand elle est réglable.
Écrire une mention générique : « vos données peuvent être traitées par des outils informatiques ». Elle ne dit ni la finalité, ni les destinataires, ni le transfert, ni l'existence d'un traitement automatisé : les articles 13 et 14 demandent ces informations, en langage clair.	Dites que l'outil d'IA aide, qu'une personne décide, citez le prestataire parmi les catégories de destinataires, le pays, la durée et l'adresse pour exercer les droits.

L'erreur, et pourquoi elle coûte	La correction
Écarter l'analyse d'impact parce que l'entreprise a moins de 250 salariés, ou la confondre avec l'évaluation de l'article 27 de l'AI Act. L'article 35 du RGPD ne dépend pas de l'effectif mais du risque : deux critères sur neuf suffisent. L'article 27 de l'AI Act vise d'autres déployeurs et ne remplace pas l'analyse d'impact.	Comptez les critères pour chaque usage, notez le décompte daté dans la fiche, et associez votre DPO ou votre conseil dès le deuxième critère.

Exercice : Mettre à jour le registre de l'agence pour le tri des demandes du site

Thomas, directeur de l'agence de communication des Chartrons (14 personnes), veut faire classer par l'offre professionnelle d'IA de l'agence les demandes reçues par le formulaire de contact du site (nom, société, courriel, téléphone, type de projet, budget, message). L'IA reçoit seulement le type de projet, le budget et le message, coordonnées masquées, et propose une catégorie ; Léa relit chaque demande et répond. L'offre a un DPA accepté le 4 novembre 2026, l'entraînement est exclu, les données sont hébergées dans l'Union. Le registre de l'agence contient déjà une ligne « Gestion des prospects et des demandes de contact ». La mention sous le formulaire dit seulement : « Vos données sont utilisées pour répondre à votre demande. » Complétez la ligne du registre, décidez de l'analyse d'impact, réécrivez la mention.

1. Dites s'il s'agit d'un nouveau traitement ou d'une ligne existante à enrichir.
2. Listez ce que l'usage ajoute à chaque rubrique de la ligne.
3. Comptez les critères d'analyse d'impact remplis et concluez.
4. Réécrivez la mention sous le formulaire, avec ce que l'article 13 demande.
5. Écrivez la demande qui fait vérifier la cohérence entre la ligne et la mention.

Le corrigé est dans le cahier d'exercices et sur la page de la leçon.

À retenir

- Toute PME qui gère une paie ou des clients tient un registre : l'exemption sous 250 salariés ne couvre pas les traitements non occasionnels, à risque ou sensibles.
- Un usage de l'IA enrichit le plus souvent la ligne d'un traitement existant : un sous-traitant, un pays, une durée, des mesures ; le registre se range par finalité, pas par outil.
- Deux critères sur neuf et l'analyse d'impact est présumée ; trier des candidatures avec une IA en coche déjà deux.
- L'évaluation de l'article 27 de l'AI Act ne vise pas une PME privée qui recrute ; l'analyse d'impact du RGPD, si.
- La mention d'information dit ce que dit le registre : le prestataire d'IA parmi les destinataires, le transfert, la durée, la décision humaine, à la collecte ou dans le mois.

03

L'AI Act, la charte et les incidents

Savoir ce que l'AI Act demande à une entreprise qui utilise l'IA, écrire la charte de l'équipe, et réagir à une demande de droits ou à une fuite.

5 Ce que l'AI Act demande à une PME qui utilise l'IA, de la formation au recrutement

6 Écrire la charte d'usage de l'IA de l'entreprise et la faire vivre

7 Répondre à une demande d'exercice de droits et réagir à une fuite de données

8 Votre plan sur 30 jours et l'évaluation finale

Leçon 5 | 38 min | Accès libre

Ce que l'AI Act demande à une PME qui utilise l'IA, de la formation au recrutement

> Une PME qui utilise ChatGPT, Copilot ou un logiciel de tri de CV est « déployeur » au sens de l'AI Act. Aujourd'hui s'appliquent la maîtrise de l'IA, les pratiques interdites et la transparence ; le 2 décembre 2027 arrivent les obligations du haut risque, dont le recrutement. Vous apprenez à ranger chaque usage et à préparer la suite.

Objectifs

- Ranger chaque usage de l'IA de l'entreprise dans l'un des quatre niveaux de risque de l'AI Act
- Rédiger la mention de transparence d'un assistant ou d'un message envoyé sans relecture
- Préparer un usage de l'IA dans le recrutement pour qu'il reste conforme aujourd'hui et au 2 décembre 2027

Le cours

La question de ce cours ne change pas : **qu'est-ce qui part, chez qui, pour quoi faire, et qui le sait ?** Le RGPD y répond pour les données. L'AI Act, le règlement européen sur l'intelligence artificielle (règlement (UE) 2024/1689), ajoute une autre question : que fait le système aux personnes qu'il touche ? Il a été modifié par le règlement (UE) 2026/1744, dit omnibus, publié au Journal officiel le 24/07/2026 et en vigueur depuis le 27/07/2026. Cette leçon dit ce que le texte demande, aujourd'hui et en 2027, à une PME qui utilise l'IA sans en fabriquer.

Déployeur ou fournisseur

L'article 3 distingue deux rôles. Le **déployeur** est l'organisation qui utilise un système d'IA sous son autorité, hors usage personnel : le cabinet RH de Mérignac qui fait résumer des CV, l'usine de Bègles qui active Microsoft 365 Copilot, l'agence des Chartrons qui génère des visuels. Le **fournisseur** développe un système d'IA, ou le fait développer, et le met sur le marché ou en service sous son nom ou sa marque : OpenAI, Anthropic, Google, Microsoft, Mistral, l'éditeur d'un logiciel de recrutement. Dans l'immense majorité des cas, votre PME est déployeur, et ce sont les obligations du déployeur qui la concernent.

Le jour où une PME devient fournisseur

Si vous faites construire un assistant sur une API et que vous l'ouvrez à vos clients sur votre site, sous votre nom, vous le mettez en service : pour cet assistant, vous êtes fournisseur au sens de l'article 3, et l'article 50 vous demande de le concevoir pour qu'il dise qu'il est une IA. Si vous installez le produit tout fait d'un éditeur, cette conception lui revient ; vérifiez qu'il la remplit avant de signer. Pour un système à haut risque, le passage au statut de fournisseur entraîne des obligations lourdes : la question se pose alors avec un juriste, avant le projet.

Le calendrier au 19 novembre 2026

Les dates de l'AI Act pour une entreprise utilisatrice

2/2/2025	2/8/2025	2/8/2026	2/12/2026	2/12/2027	2/8/2028
Interdictions et maîtrise de l'IA	**Modèles à usage général**	**Transparence**	**Neuvième interdiction**	**Haut risque de l'annexe III**	**Haut risque de l'annexe I**
Huit pratiques interdites ; article 4 sur la formation du personnel.	Obligations des éditeurs de modèles, pas des PME qui s'en servent.	Dire qu'une IA répond, signaler un hypertrucage.	Images intimes sans consentement et contenus pédocriminels.	Recrutement, gestion des salariés, crédit aux particuliers.	IA intégrée à des produits réglementés, comme les machines.

Calendrier relu le 19/11/2026 sur la page de la Commission européenne, après l'omnibus entré en vigueur le 27/07/2026.

Trois blocs de règles s'appliquent **déjà** à votre entreprise : l'article 4 sur la maîtrise de l'IA et l'article 5 sur les pratiques interdites, depuis le 2/2/2025, et l'article 50 sur la transparence, depuis le 2/8/2026. Le 2/12/2026, dans moins de deux semaines, une neuvième interdiction entre en application. Les obligations des usages à haut risque de l'annexe III, dont le recrutement, ont été reportées par l'omnibus au **2/12/2027**. Ce report ne touche pas le RGPD, qui continue de s'appliquer en entier.

Quatre niveaux de risque

Les quatre niveaux de risque

Pratiques interdites

Article 5 : huit pratiques depuis le 2/2/2025, une neuvième au 2/12/2026. Ne pas les utiliser, même avec l'accord des personnes.

Haut risque

Annexe III : recrutement, décisions sur les salariés, crédit aux particuliers. Obligations du déployeur au 2/12/2027 (article 26).

Transparence

Article 50 : dire qu'une IA répond, signaler une image, un son ou une vidéo qui imite le réel. Depuis le 2/8/2026.

Risque minimal

Résumer, traduire, rédiger un brouillon relu. Aucune règle nouvelle, en dehors de l'article 4 et du RGPD.

Du plus grave au plus courant. La plupart des usages d'une PME se rangent dans la dernière couche.

Dix usages courants d'une PME rangés par niveau

Usage	Niveau	Pourquoi	Ce que vous faites
Résumer le compte rendu d'une réunion de production avec Copilot	Minimal	Aucune décision sur une personne	RGPD et charte ; aucune règle nouvelle
Préparer un brouillon de réponse à un client, relu avant l'envoi	Minimal	La réponse relue et envoyée par une personne est la sienne	Relecture maintenue
Traduire une notice technique en espagnol	Minimal	Aucun échange direct, aucune décision	Relecture des termes techniques
Assistant du site qui répond seul aux visiteurs	Transparence	Une personne échange directement avec une IA	Mention claire au premier message
Vidéo de vœux avec la voix clonée du gérant	Transparence	Hypertrucage : un son qui imite une personne réelle	Mention « voix générée par IA »

Usage	Niveau	Pourquoi	Ce que vous faites
Article sur une réforme fiscale publié sans aucune relecture	Transparence	Texte généré publié pour informer le public sur une question d'intérêt public	Relecture humaine et responsabilité éditoriale, ou mention
Logiciel qui note et classe les candidatures	Haut risque	Annexe III, point 4 a : tri des candidatures	Une personne décide ; article 22 du RGPD dès aujourd'hui
Planning qui répartit les postes selon le comportement de chacun	Haut risque	Annexe III, point 4 b : répartition des tâches selon le comportement	Une personne valide ; CSE informé
Score de solvabilité de clients particuliers	Haut risque	Annexe III, point 5 b, hors détection de fraude	Une personne décide ; juriste consulté
Caméra qui déduit l'humeur des opérateurs	Interdit	Article 5, point f : émotions sur le lieu de travail	Refuser le dispositif

Où se range cet usage

1 **L'outil s'abstient-il de déduire les émotions d'un salarié ou d'un candidat, ou sa religion, ses opinions, son orientation à partir de son visage ou de sa voix ?**

Non Pratique interdite : ne pas l'utiliser, ou faire retirer la fonction.

2 **L'outil reste-t-il en dehors du tri des candidatures, des décisions sur les salariés et de la solvabilité des particuliers ?**

Non

Haut risque au 2/12/2027 ; article 22 du RGPD dès aujourd'hui : une personne décide.

3 **Une personne relit-elle ce qui part vers un client ou vers le public ?**

Non Transparence : dire que c'est une IA, au plus tard au premier échange.

4 **Le contenu produit évite-t-il d'imiter une personne, un lieu ou un fait réels ?**

Non Hypertrucage : le signaler comme généré ou modifié par une IA.

Oui à tout **Risque minimal : article 4, RGPD et charte d'usage.**

Posez les questions dans l'ordre : la première réponse « non » donne le niveau et la conduite à tenir.

Demande à recopier **Ranger les usages de votre registre**

```
Rôle : tu aides une PME de [effectif] salariés, secteur [secteur], à ranger ses usages de l'IA selon l'AI Act. Tu ne donnes pas d'avis juridique.
Contexte : voici la liste de nos usages, une ligne par usage (ce que fait l'outil, qui reçoit le résultat, relecture humaine oui ou non). Elle ne contient aucune donnée personnelle : [collez la liste].
Tâche : pour chaque usage, propose un niveau parmi : pratique interdite (article 5), haut risque (annexe III), transparence (article 50), risque minimal. Justifie en une phrase en citant le critère : émotions ou catégorisation biométrique, recrutement, décision sur un salarié, solvabilité d'un particulier, échange direct avec une IA, contenu qui imite le réel, aucune décision sur une personne.
Format : un tableau de quatre colonnes (usage, niveau, critère, ce qui change). Puis une liste « À faire examiner » pour tout usage dont le niveau dépend d'un détail absent de la ligne.
```

Ce que vous devez obtenir : Un tableau d'une ligne par usage et deux ou trois lignes « À faire examiner », du type « Planning de l'atelier : dépend de ce que mesure l'outil ; s'il répartit selon le comportement individuel, haut risque ». Ce tableau est un premier tri : chaque niveau se relit avec l'arbre de la leçon.

Note : La liste décrit des usages, pas des personnes : elle peut aller dans l'offre professionnelle de l'entreprise.

Les pratiques interdites d'une entreprise ordinaire

L'article 5 liste huit pratiques interdites depuis le 2/2/2025 : manipulation qui cause un préjudice important, exploitation de la vulnérabilité liée à l'âge, au handicap ou à la situation sociale, notation sociale, prédiction d'infraction fondée sur le seul profilage, moissonnage non ciblé de visages, **reconnaissance des émotions sur le lieu de travail et dans l'enseignement** (sauf raisons médicales ou de sécurité), **catégorisation biométrique** qui déduit l'origine, les opinions politiques, l'appartenance syndicale, la religion, la vie ou l'orientation sexuelle, et identification biométrique en temps réel par les forces de l'ordre. Les deux pratiques en gras sont celles qu'un fournisseur peut proposer à une PME, sous le nom de « bien-être », d'« engagement » ou d'« analyse d'entretien ». L'accord des salariés n'y change rien : une pratique interdite le reste. Le considérant 18 du règlement précise que des états physiques comme la douleur ou la fatigue ne sont pas des émotions : détecter la somnolence d'un cariste pour éviter un accident n'est pas visé par cette interdiction, mais reste soumis au RGPD et au Code du travail. L'omnibus a ajouté une neuvième interdiction, en deux points, applicable le 2/12/2026 : générer des images intimes ou sexuelles réalistes d'une personne identifiable sans son consentement explicite, et des contenus pédocriminels.

La transparence depuis le 2 août 2026

L'article 50 pose trois règles qui touchent une PME. Un système qui échange directement avec des personnes est conçu pour qu'elles sachent qu'elles parlent à une IA, sauf si c'est évident pour une personne raisonnablement informée. Le déployeur signale un **hypertrucage**, c'est-à-dire une image, un son ou une vidéo générés ou modifiés qui ressemblent à des personnes, des lieux ou des faits réels et pourraient passer pour authentiques ; pour une œuvre manifestement artistique ou satirique, la mention est allégée. Le déployeur signale aussi un texte généré publié pour informer le public sur une question d'intérêt public, sauf s'il a été relu par une personne et qu'une personne ou une entreprise en porte la responsabilité éditoriale. L'information est claire, distincte, et donnée **au plus tard lors de la première interaction ou exposition**. Le marquage technique des contenus générés incombe aux fournisseurs ; son détail est traité dans « L'article 50 de l'AI Act, les mentions, le marquage C2PA et les étiquettes des réseaux ».

Demande à recopier **Rédiger la mention de transparence d'un assistant ou d'un message automatique**

```
Rôle : tu rédiges des messages clairs pour une PME de [secteur] à [ville].
Contexte : nous utilisons [décrivez l'outil : assistant sur le site qui répond seul /
réponse automatique envoyée sans relecture]. Il sait répondre sur [sujets]. Il ne sait
pas répondre sur [sujets exclus]. Une personne de l'équipe est joignable au [téléphone]
ou à [adresse électronique], [horaires].
Tâche : écris le premier message de l'assistant, ou la première phrase du message
automatique, qui dit clairement qu'il s'agit d'un programme d'intelligence
artificielle, ce qu'il sait faire et comment joindre une personne.
```

```
Format : quatre lignes au plus, vouvoiement, la mention en première phrase, aucun
prénom humain pour signer, aucune promesse de prix, de délai ou de disponibilité.
```

Ce que vous devez obtenir : « Bonjour, je suis l'assistant automatique de [entreprise], un programme d'intelligence artificielle. Je réponds aux questions sur [sujets]. Pour [sujets exclus], une personne de l'équipe vous répond au [téléphone], [horaires]. » La mention vient avant tout contenu, dans la langue du visiteur.

Note : Un brouillon relu, corrigé et envoyé par un salarié est sa réponse : il n'a pas besoin de cette mention.

Le recrutement, premier haut risque des PME

L'annexe III, point 4, vise les systèmes destinés au recrutement et à la sélection (annonces ciblées, analyse et filtrage des candidatures, évaluation des candidats), aux décisions sur les relations de travail (promotion, rupture, répartition des tâches selon le comportement ou les traits personnels) et au suivi des performances. À partir du 2/12/2027, l'article 26 demandera au déployeur d'utiliser le système selon sa notice, de confier le contrôle humain à des personnes compétentes, formées et dotées de l'autorité nécessaire, de veiller à la pertinence des données d'entrée qu'il maîtrise, de surveiller le fonctionnement et de suspendre en cas de risque, de garder les journaux au moins six mois, d'informer les représentants du personnel et les salariés concernés **avant** la mise en service au travail, et d'informer les personnes qui font l'objet d'une décision. Trois règles s'appliquent déjà : l'article 22 du RGPD, qui interdit sauf exceptions une décision fondée exclusivement sur un traitement automatisé qui affecte significativement une personne ; l'article L1221-9 du Code du travail, selon lequel aucune information sur un candidat ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance ; et, dans les entreprises d'au moins 50 salariés, l'information et la consultation du comité social et économique sur l'introduction de nouvelles technologies (article L2312-8). La position du cours est nette : **une IA ne trie jamais seule des candidatures**.

L'IA dans un recrutement de PME

Ce que l'IA peut faire

- Rédiger l'annonce à partir de la fiche de poste
- Préparer une grille d'entretien identique pour tous
- Résumer un CV pseudonymisé selon cette grille
- Signaler une pièce manquante au dossier

Ce qu'elle ne fait pas

- Noter, classer ou écarter un candidat
- Choisir qui passe en entretien
- Analyser la voix ou le visage en entretien vidéo
- Envoyer seule une réponse négative

La colonne de gauche aide la personne qui recrute ; celle de droite décide à sa place.

Demande à recopier **Préparer la note d'information aux salariés avant un outil d'aide au recrutement**

```
Rôle : tu aides la direction d'une PME de [effectif] salariés à informer son personnel,
en langage clair et sans jargon.
Contexte : nous allons utiliser [outil, offre professionnelle sous contrat] pour [usage
précis : résumer les CV pseudonymisés selon une grille, rédiger les annonces]. L'outil
ne note, ne classe et n'écarte aucun candidat : [prénom et fonction] lit chaque
candidature et décide. Les données passent chez [éditeur], sous-traitant, hébergées
[lieu]. Mise en service prévue le [date]. Référent : [prénom, fonction].
Tâche : rédige la note d'information aux salariés et, si l'entreprise en a, aux
représentants du personnel, à diffuser avant la mise en service.
Format : une page au plus, cinq rubriques (ce qui change, ce que l'outil fait, ce qu'il
ne fait pas, qui décide, à qui poser vos questions), phrases courtes. N'invente aucune
règle, aucune date et aucun article de loi.
```

Ce que vous devez obtenir : Une note d'une page en cinq rubriques, qui reprend vos éléments sans rien ajouter et dit en toutes lettres qu'aucune candidature n'est écartée par un programme. Vérifiez les crochets un par un avant la diffusion, et datez l'envoi.

L'article 4 et les sanctions

L'article 4 a été réécrit par l'omnibus : fournisseurs et déployeurs **prennent des mesures pour soutenir le développement de la maîtrise de l'IA** de leur personnel et des personnes qui utilisent les systèmes pour leur compte, en tenant compte de leurs connaissances et du contexte d'usage. Le texte précise qu'il n'exige pas de garantir un niveau précis à chaque personne. Les mesures les plus simples à montrer : la liste de qui utilise quels outils, la formation suivie par chacun avec sa date, une charte d'usage, l'objet de la leçon « Écrire la charte d'usage de l'IA de l'entreprise et la faire vivre ». Les amendes de l'article 99 vont jusqu'à 35 M€ ou 7 % du chiffre d'affaires annuel mondial pour une pratique interdite, 15 M€ ou 3 % pour les autres obligations, dont celles des articles 26 et 50, et 7,5 M€ ou 1 % pour des informations inexactes fournies aux autorités. Pour une PME, c'est le **plus bas** des deux montants qui sert de plafond.

> **Notre position**
>
> Pour neuf usages sur dix d'une PME, l'AI Act ne demande rien de plus que ce que ce cours conseille déjà : une équipe formée, une charte, une relecture humaine de ce qui part. Le dixième, celui qui touche un candidat, un salarié ou le crédit d'un particulier, se règle maintenant, pas en novembre 2027. Ajoutez une colonne « niveau AI Act » à la ligne du registre décrite dans « Inscrire un usage de l'IA au registre et informer les personnes concernées ».

Les erreurs fréquentes

L'erreur, et pourquoi elle coûte	La correction
Penser que l'AI Act ne concerne que les éditeurs comme OpenAI ou Mistral, et ne rien faire. Le texte vise aussi les déployeurs : l'article 4 sur la maîtrise de l'IA, l'article 5 sur les pratiques interdites et l'article 50 sur la transparence s'appliquent déjà à une PME qui utilise l'IA.	Rangez vos usages avec l'arbre de la leçon, notez le niveau sur la ligne du registre, et documentez la formation de l'équipe.
Garder un tri automatique des candidatures « puisque le haut risque ne s'applique qu'au 2 décembre 2027 ». Le report touche les obligations de l'AI Act, pas le RGPD : l'article 22 encadre dès aujourd'hui une décision fondée exclusivement sur un traitement automatisé qui affecte significativement une personne.	Retirez tout score qui écarte ou masque des candidatures : l'outil extrait ou résume, une personne lit et décide, et l'annonce le dit.
Accepter un outil de « bien-être » qui lit les émotions des salariés parce qu'ils ont tous signé leur accord. La reconnaissance des émotions sur le lieu de travail est une pratique interdite par l'article 5, sauf raisons médicales ou de sécurité. Le consentement ne lève pas une interdiction.	Refusez la fonction par écrit, en citant l'article 5, point f. Si l'objectif est la sécurité, cherchez un dispositif qui détecte un état physique, comme la somnolence, et traitez-le avec le CSE et le RGPD.
Placer la mention « assistant automatique » dans les conditions générales du site et donner à l'assistant un prénom humain. L'article 50 demande une information claire et distincte au plus tard lors de la première interaction. Personne ne lit les conditions générales avant de poser une question, et un prénom fait croire à une personne.	Écrivez la mention dans la première phrase de l'assistant, avec un moyen de joindre une personne, et retirez le prénom.

Exercice : Ranger les huit usages du cabinet comptable de Libourne

Nathalie, associée expert-comptable du cabinet de Libourne (22 personnes), prépare la réunion des associés de décembre. Julien a recensé huit usages, en place ou proposés : 1. résumer les notes de rendez-vous client avec l'offre professionnelle sous contrat du cabinet, relues par le collaborateur ; 2. un assistant sur le site qui répondrait seul aux questions des prospects sur la tenue comptable et les tarifs ; 3. un module proposé par un éditeur qui note la « productivité » de chaque collaborateur à partir du temps passé par dossier et suggère le montant des primes ; 4. un logiciel qui attribue un score aux candidatures d'alternants et masque celles sous 50 sur 100 ; 5. la lettre d'information mensuelle aux clients sur les nouveautés fiscales, rédigée avec une IA et relue par Nathalie qui la signe ; 6. un outil qui calcule pour des clients particuliers un score d'emprunteur transmis à leur banque ; 7. une option du logiciel de visioconférence qui mesure l'« enthousiasme » des participants aux réunions d'équipe par l'analyse du visage ; 8. une vidéo de présentation du cabinet où un avatar généré reprend l'image et la voix de Nathalie, qui l'a autorisé. Rangez chaque usage et dites ce qui change.

1. Passez chaque usage dans l'arbre « Où se range cet usage » et notez la question qui le décide.

2. Pour chaque usage qui n'est pas au risque minimal, écrivez ce qui change dans sa mise en œuvre.
3. Rédigez la mention de l'usage 2 et celle de l'usage 8.
4. Listez les mesures de l'article 4 que le cabinet peut montrer, et deux questions à poser à un juriste.

Le corrigé est dans le cahier d’exercices et sur la page de la leçon.

À retenir

- Une PME qui utilise l'IA est déployeur ; elle devient fournisseur si elle met en service sous son nom un système qu'elle a fait construire.
- Aujourd'hui s'appliquent l'article 4 (maîtrise de l'IA), l'article 5 (pratiques interdites) et l'article 50 (transparence) ; la neuvième interdiction arrive le 2/12/2026.
- Lire les émotions des salariés ou des candidats est interdit, même avec leur accord ; détecter la fatigue pour la sécurité ne l'est pas.
- Le recrutement est à haut risque au 2/12/2027, mais l'article 22 du RGPD et l'article L1221-9 du Code du travail s'appliquent déjà : une IA ne trie jamais seule.
- Un assistant qui répond seul dit qu'il est une IA au premier message ; un hypertrucage se signale toujours.

Leçon 6 | 34 min | Accès libre

Écrire la charte d'usage de l'IA de l'entreprise et la faire vivre

> Une charte interne qui fixe les usages autorisés et interdits de l'IA est la première mesure à montrer pour l'article 4 de l'AI Act. Vous écrivez une charte de deux pages en sept parties, vous la faites valider selon l'effectif de l'entreprise, puis vous la faites vivre : présentation, formation datée, relecture tous les six mois.

Objectifs

- Rédiger la charte d'usage de l'IA de votre entreprise en sept parties, sur deux pages au plus
- Choisir la procédure de validation qui convient à votre effectif et à vos représentants du personnel
- Organiser la présentation, la formation et la relecture de la charte, preuves datées à l'appui

Le cours

Qu'est-ce qui part, chez qui, pour quoi faire, et qui le sait ? Une charte d'usage de l'IA répond à cette question une fois pour toute l'équipe, au lieu de laisser chacun y répondre seul devant son écran. La Commission nationale de l'informatique et des libertés (CNIL), dans ses questions-réponses du 18/07/2024 sur l'IA générative, recommande d'encadrer ces outils par des « politiques ou chartes internes, définissant clairement les usages autorisés et les usages interdits », de former les utilisateurs « de façon adaptée » et de mener des contrôles réguliers. La charte est aussi la première pièce à montrer pour l'article 4 de l'AI Act, le règlement européen sur l'intelligence artificielle, qui demande à l'entreprise de prendre des mesures pour soutenir la maîtrise de l'IA de son personnel.

Ce que la charte doit régler

Les sept parties d'une charte de PME

1. Outils et comptes
Quels outils, quelles offres, quels comptes ? Comptes professionnels seulement.

2. Données
Ce qui peut partir, ce qui se pseudonymise avant, ce qui ne part jamais.

3. Usages
Autorisés, soumis à validation, interdits, dont les pratiques de l'article 5 de l'AI Act.

4. Relecture et responsabilité
Qui relit ce qui sort, et qui en répond.

5. Transparence
Ce qui est dit aux clients et au public quand une IA a produit ou répond.

6. Formation et référent
Qui est formé, quand, et à qui poser ses questions.

7. Doute ou incident
Qui prévenir, en combien de temps, et ce qu'il ne faut pas faire.

Deux pages au plus. Chaque partie répond à une question qu'un salarié se pose devant son écran.

Chaque partie s'appuie sur une règle déjà vue dans ce cours. Les outils et les comptes renvoient au contrat de sous-traitance de l'article 28 du RGPD : un compte personnel gratuit n'en a pas, et la CNIL recommande de désactiver la réutilisation des données par le fournisseur quand c'est possible. Les données reprennent les trois couleurs de la leçon « Ce qui devient une donnée personnelle quand vous écrivez à une IA » et le principe de minimisation de l'article 5. Les usages interdits reprennent les pratiques de l'article 5 de l'AI Act et l'article 22 du RGPD sur la décision automatisée. La transparence

applique l'article 50 de l'AI Act. La formation documente l'article 4. La conduite en cas d'incident prépare les 72 heures de l'article 33 du RGPD.

La charte de l'agence des Chartrons partie par partie

Partie	Ce que dit la charte	Exemple concret	Ce qui la fonde
1. Outils et comptes	Seule l'offre professionnelle sous contrat de l'agence, avec des comptes nominatifs créés par Thomas ; aucun compte personnel pour le travail	Léa ferme son compte gratuit et recrée ses gabarits dans l'espace de l'agence	RGPD, article 28 ; CNIL, 18/07/2024
2. Données	Vert : textes publics, chiffres agrégés. Orange : contacts et verbatims de clients, pseudonymisés avant l'envoi. Rouge : santé, RIB, pièces d'identité, mineurs	Les verbatims d'enquête partent avec [Répondant 12] à la place des noms	RGPD, articles 5 et 9
3. Usages	Autorisés, sous validation de Léa sous 48 heures, interdits (voir le schéma)	Le visuel réaliste d'un chef généré pour un client attend la validation de Léa	AI Act, articles 5 et 50 ; RGPD, article 22
4. Relecture et responsabilité	Tout contenu qui sort de l'agence est relu par une personne qui en répond ; chaque chiffre et chaque source sont vérifiés	La plaquette d'un client est relue par Léa, les chiffres par le chargé de compte	Responsabilité de l'agence envers ses clients
5. Transparence	Mention sur toute image ou voix réaliste générée ; tout assistant qui répond seul dit qu'il est une IA	« Image générée par intelligence artificielle » sous le visuel	AI Act, article 50
6. Formation et référent	Référente IA : Léa. Formation de deux heures pour chacun, datée ; nouvel arrivant formé dans le mois	Le registre des formations est tenu par Thomas	AI Act, article 4
7. Doute ou incident	Prévenir Léa ou Thomas dans l'heure ; ne rien supprimer avant leur avis	Un fichier client collé par erreur, signalé à 10 h, traité le jour même	RGPD, article 33

Les usages de l'agence en trois couleurs

Autorisé

- Reformuler un texte de l'agence
- Résumer un document public
- Chercher des idées de titres
- Traduire une plaquette, puis la faire relire

Sous validation du référent, sous 48 heures

- Visuel réaliste ou voix générée
- Assistant qui répond seul à des clients
- Nouvel outil ou nouveau connecteur
- Données d'un client, pseudonymisées

Interdit

- Compte personnel gratuit pour le travail
- Donnée sensible, RIB ou pièce d'identité
- Décision sur un candidat ou un salarié
- Lire les émotions d'une personne

Exemple tiré de la charte de l'agence des Chartrons. La colonne orange désigne une personne qui valide, et un délai.

La colonne orange fait la différence entre une charte qui sert et une charte qui bloque. Elle nomme **une personne** qui valide et **un délai** : « Léa, sous 48 heures ». Sans elle, tout ce qui n'est pas clairement autorisé devient interdit dans l'esprit des salariés, et l'usage part sur les téléphones personnels, hors de toute règle. La colonne rouge, elle, reste courte : quatre à six interdits, chacun compréhensible sans connaître le RGPD.

Écrire la charte en une heure

Commencez par répondre vous-même à dix questions, sans IA : l'effectif ; les outils et les offres utilisés ; les comptes (qui les crée, qui les ferme) ; les données que manipule l'entreprise ; celles qui ne doivent jamais partir ; les usages fréquents ; les usages sensibles ; ce que vous dites aux clients ; le nom du référent ; la conduite en cas d'incident. Ces réponses décrivent l'entreprise, pas des personnes : elles

peuvent aller dans l'offre professionnelle de l'entreprise. L'IA met en forme ; c'est vous qui décidez de chaque règle.

Demande à recopier **Rédiger la charte à partir de dix réponses**

```
Rôle : tu rédiges des documents internes clairs pour une PME, sans jargon juridique.
Contexte : voici nos dix réponses.
1. Effectif et activité : [nombre] personnes, [secteur], [ville].
2. Outils et offres : [outil, offre professionnelle ou non, contrat signé oui ou non].
3. Comptes : [qui les crée, qui les ferme au départ d'un salarié].
4. Données que nous manipulons : [catégories, sans exemple réel].
5. Données qui ne partent jamais : [catégories].
6. Usages fréquents : [liste].
7. Usages sensibles : [liste].
8. Ce que nous disons aux clients : [règle].
9. Référent IA : [prénom, fonction] ; délai de validation : [délai].
10. En cas d'incident : [qui prévenir, en combien de temps].
Tâche : rédige la charte d'usage de l'IA en sept parties : outils et comptes ; données (autorisées, à pseudonymiser, interdites) ; usages (autorisés, soumis à validation, interdits) ; relecture et responsabilité ; transparence ; formation et référent ; doute ou incident.
Format : deux pages au plus, phrases courtes, « vous » pour s'adresser au salarié.
Reprends mes réponses sans rien ajouter : aucune règle, aucun outil et aucun article de loi que je n'ai pas donnés. Termine par une liste « À préciser » de ce qui manque pour que la charte soit applicable.
```

Ce que vous devez obtenir : Une charte en sept titres numérotés, chaque règle tirée de vos réponses, et une liste « À préciser » de deux à cinq points, par exemple « Délai de validation : qui remplace le référent pendant ses congés ? ». Relisez chaque phrase en vous demandant : un salarié saurait-il quoi faire demain matin ?

Ce que l'IA ajoute si vous la laissez faire

Sans la consigne « aucun article de loi que je n'ai pas donné », une charte générée cite volontiers des articles inventés ou périmés, comme l'ancienne formule de l'article 4 qui demandait de « garantir un niveau suffisant » de maîtrise de l'IA, réécrite par l'omnibus de juillet 2026. **Une charte qui cite un texte faux perd sa crédibilité dès la première question d'un salarié.**

Demande à recopier **Produire la version d'une page et le quiz de compréhension**

```
Voici notre charte d'usage de l'IA validée par la direction : [collez la charte].
Tâche 1 : écris la version d'une page à afficher près des postes : les trois couleurs d'usages, les trois couleurs de données, le nom du référent et la conduite en cas d'incident.
Tâche 2 : écris un quiz de cinq questions de mise en situation, trois réponses possibles chacune, une seule bonne, avec la bonne réponse et une phrase d'explication tirée de la charte.
Format : n'invente aucune règle absente de la charte. Les situations du quiz sont celles de notre métier : [métier].
```

Ce que vous devez obtenir : Une page en quatre blocs, lisible debout devant un écran, et cinq questions du type « Un client vous envoie la photo de sa carte d'identité pour un dossier : pouvez-vous la joindre à une demande à l'IA pour en extraire les informations ? ». Chaque explication renvoie à une partie de la charte.

Sa valeur dans le droit du travail

Dans une entreprise d'au moins 50 salariés, le règlement intérieur est obligatoire (article L1311-2 du Code du travail). Les notes de service et autres documents qui posent des obligations générales et permanentes dans les matières du règlement intérieur, dont la discipline, en sont des adjonctions (article L1321-5) : la charte suit alors la même procédure, avis du comité social et économique, communication à l'inspection du travail avec cet avis, et entrée en vigueur un mois au moins après les formalités de publicité (article L1321-4). En dessous de 50 salariés, la charte se diffuse le plus souvent comme une note de service datée, présentée en réunion et accompagnée d'un accusé de lecture. Si elle prévoit un contrôle individuel de l'usage des outils, l'article L1222-4 impose d'informer chaque salarié avant la mise en place du dispositif. La valeur d'une charte pour fonder une sanction dépend de sa procédure d'adoption : faites-la relire par un juriste en droit social si vous comptez vous en servir ainsi.

Quelle procédure pour votre charte

1 **L'entreprise compte-t-elle moins de 50 salariés ?**

Non

Règlement intérieur obligatoire (L1311-2) : la charte qui impose des règles générales et permanentes en est une adjonction (L1321-5), avec avis du CSE et communication à l'inspection du travail (L1321-4).

2 **La charte se limite-t-elle à des règles d'usage, sans dispositif qui collecte des informations sur chaque salarié ?**

Non

Chaque salarié est informé du dispositif avant sa mise en place (L1222-4), et le CSE s'il existe.

Oui à tout **Note de service datée, présentée en réunion, accusé de lecture de chacun.**

Code du travail relu le 19/11/2026. Si la charte doit fonder une sanction disciplinaire, faites-la relire par un juriste en droit social.

La faire vivre

La vie d'une charte

1 — Rédiger

Dix réponses, deux pages, relues par la direction.

2 — Présenter

Trente minutes en réunion, questions, accusé de lecture.

3 — Former

Formation datée, quiz de cinq questions, nouvel arrivant dans le mois.

4 — Relire

Tous les six mois et à chaque nouvel outil, nouvelle version datée.

Un tour complet tous les six mois, et un tour accéléré à chaque nouvel outil.

Une présentation de 30 minutes suffit : dix minutes sur les trois couleurs, dix sur deux cas concrets du métier, dix de questions. Chacun signe ou envoie un accusé de lecture, et passe le quiz de cinq questions. Le référent tient le registre des formations, une ligne par personne, avec la date. La charte se relit tous les six mois et à chaque nouvel outil ; chaque version porte sa date en pied de page. Ces quatre preuves, charte datée, accusés de lecture, registre des formations, versions successives, sont exactement ce que l'article 4 demande de pouvoir montrer.

Le registre des formations de l'agence

Date	Personne	Formation	Durée	Quiz	Prochaine relecture
12/01/2027	Léa, cheffe de projet, référente	Présentation de la charte et cas de l'agence	2 h	5 sur 5	12/07/2027
12/01/2027	Hugo, graphiste	Présentation de la charte et cas de l'agence	2 h	4 sur 5, question 3 reprise	12/07/2027
03/02/2027	[nouvel arrivant]	Charte, puis accompagnement par Léa	1 h 30	[score]	12/07/2027

Notre position

Mieux vaut une charte de deux pages appliquée qu'une charte de vingt pages signée et oubliée. Cette leçon va plus loin que les chartes de « Déployer ChatGPT dans l'équipe : la charte d'usage, l'AI Act et le RGPD » et de « L'AI Act après l'omnibus de 2026 et la charte d'usage de l'équipe », parce qu'elle vaut pour tous les outils et relie chaque règle à son article. Si vous n'en gardez qu'une partie, gardez la septième : un salarié qui sait qui prévenir dans l'heure transforme une fuite en incident maîtrisé.

Les erreurs fréquentes

L'erreur, et pourquoi elle coûte	La correction
Reprendre la charte de vingt pages d'un grand groupe trouvée en ligne. Elle parle d'outils, de services et de procédures que la PME n'a pas. Personne ne la lit, et les règles utiles, celles des données que l'équipe manipule vraiment, n'y figurent pas.	Partez de vos dix réponses et des sept parties. Deux pages, avec vos outils, vos données et le nom de votre référent.
Interdire toute IA dans l'entreprise pour être tranquille. L'usage continue sur les téléphones et les comptes personnels, sans contrat ni réglage, là où les données sont le moins protégées. L'interdiction générale déplace le risque au lieu de le réduire.	Autorisez un outil professionnel sous contrat, écrivez les interdits précis, et donnez une voie de validation avec un nom et un délai.
Faire signer la charte une fois, puis ne plus jamais l'ouvrir. Au bout de six mois, les outils listés ont changé, un connecteur a été ajouté, un nouvel arrivant ne l'a jamais vue. La charte ne protège plus rien et ne prouve plus aucune mesure.	Inscrivez la relecture semestrielle à l'agenda du référent, relisez à chaque nouvel outil et datez chaque version.
Diffuser la charte générée par une IA sans la relire phrase par phrase. Elle peut contenir des règles que l'entreprise n'a jamais décidées, des outils qu'elle n'utilise pas ou des articles de loi inventés ou périmés.	Exigez dans la demande « aucune règle ni aucun article que je n'ai pas donnés », puis relisez chaque phrase en vous demandant si vous l'avez décidée.

Exercice : Écrire la charte du cabinet RH de Mérignac

Karim, gérant du cabinet RH de Mérignac (9 personnes, sans représentants du personnel), veut une charte avant la fin de l'année. Voici ses dix réponses. 1. Cabinet de recrutement et de conseil RH, 9 personnes. 2. Une offre professionnelle d'IA sous contrat, entraînement exclu, et Microsoft 365. 3. Comptes créés et fermés par Karim. 4. CV, lettres, notes d'entretien, résultats de tests de personnalité, coordonnées de clients. 5. Ne partent jamais : santé, handicap, situation familiale, origine, pièces d'identité, résultats bruts de tests. 6. Usages fréquents : annonces, comptes rendus d'entretien à partir de notes pseudonymisées, courriels aux clients. 7. Usages sensibles : résumé de CV, synthèse d'un entretien pour le client. 8. Les candidats sont informés dans les annonces qu'un outil d'IA aide à lire les candidatures. 9. Référente : Sophie, validation sous 24 heures. 10.

Incident : prévenir Karim dans l'heure. Rédigez la charte en sept parties et choisissez sa procédure de diffusion.

1. Classez les données du point 4 en vert, orange et rouge.
2. Rangez les usages des points 6 et 7 en autorisés, sous validation, interdits, et ajoutez les interdits que le cabinet doit écrire noir sur blanc.
3. Rédigez les sept parties en deux pages au plus.
4. Choisissez la procédure de diffusion avec l'arbre « Quelle procédure pour votre charte ».

Le corrigé est dans le cahier d’exercices et sur la page de la leçon.

À retenir

- La CNIL recommande une charte interne qui définit clairement les usages autorisés et interdits de l'IA ; c'est la première preuve des mesures de l'article 4.
- Sept parties, deux pages : outils et comptes, données, usages, relecture, transparence, formation et référent, doute ou incident.
- La colonne « sous validation » nomme une personne et un délai ; sans elle, l'usage part sur les téléphones personnels.
- À partir de 50 salariés, une charte qui impose des obligations générales et permanentes suit la procédure du règlement intérieur, avec l'avis du CSE.
- Charte datée, accusés de lecture, registre des formations, relecture tous les six mois et à chaque nouvel outil : ce sont vos preuves.

Leçon 7 | 36 min | Accès libre

Répondre à une demande d'exercice de droits et réagir à une fuite de données

> Une personne peut demander ce que vous avez fait de ses données, IA comprise : vous répondez en un mois, gratuitement, en cherchant aussi dans les conversations et chez le sous-traitant. Une fuite se confine dans l'heure, se documente toujours, se notifie sous 72 heures si le risque n'est pas improbable, et s'annonce aux personnes s'il est élevé.

Objectifs

- Traiter une demande d'accès, d'effacement ou d'opposition dans le délai d'un mois, conversations d'IA comprises
- Décider, après un incident, s'il faut notifier la Commission nationale de l'informatique et des libertés (CNIL) et informer les personnes
- Rédiger l'accusé de réception, la notification et le message aux personnes concernées en langage clair

Le cours

Qu'est-ce qui part, chez qui, pour quoi faire, et qui le sait ? Deux situations obligent à répondre à cette question dans un délai fixé par la loi. Une personne vous écrit pour savoir ce que vous avez fait de ses données, et parfois si une IA les a lues. Ou des données s'échappent : un fichier collé dans un compte gratuit, un lien de partage public, un connecteur trop large. La CNIL contrôle les deux. Cette leçon vous donne la marche à suivre, heure par heure pour la fuite, jour par jour pour la demande.

Les droits que vos clients, candidats et salariés exercent

Les droits des articles 15 à 22 quand une IA est passée par là

Droit	Ce que la personne demande	Ce que l'IA change pour vous
Accès et copie (article 15)	Savoir si ses données sont traitées, pourquoi, par qui, combien de temps, d'où elles viennent, et en obtenir une copie	Les conversations, les fichiers envoyés et l'éditeur, destinataire en tant que sous-traitant, font partie de la réponse
Rectification (article 16)	Corriger une donnée inexacte	Un résumé généré qui contient une erreur sur la personne se corrige aussi
Effacement (article 17)	Faire supprimer ses données qui ne sont plus nécessaires, ou après retrait du consentement	Supprimer aussi la conversation et les fichiers chez l'éditeur ; exceptions : obligation légale, défense en justice

Droit	Ce que la personne demande	Ce que l'IA change pour vous
Limitation (article 18)	Geler l'usage de ses données pendant une vérification	Ne plus envoyer ces données à l'IA pendant ce temps
Portabilité (article 20)	Récupérer ses données dans un format réutilisable, quand le traitement repose sur son consentement ou un contrat et qu'il est automatisé	Rarement en jeu pour un usage d'assistant
Opposition (article 21)	S'opposer au traitement ; sans condition pour la prospection	Un fichier de prospection enrichi par une IA perd la personne, à tout moment
Décision automatisée (article 22)	Ne pas subir une décision fondée exclusivement sur un traitement automatisé qui l'affecte significativement	Droit d'obtenir une intervention humaine, d'exprimer son point de vue, de contester

L'article 12 fixe les règles du jeu. Vous répondez **dans un délai d'un mois** à compter de la réception de la demande ; ce délai peut être prolongé de deux mois si la demande est complexe ou si les demandes sont nombreuses, à condition d'en informer la personne dans le premier mois, avec les motifs. La réponse est **gratuite** ; seule une demande manifestement infondée ou excessive permet de demander des frais raisonnables ou de refuser, et c'est à vous de le démontrer. Vous ne demandez une pièce supplémentaire pour vérifier l'identité qu'en cas de doute raisonnable : un candidat qui écrit depuis l'adresse électronique de sa candidature n'a pas à envoyer sa carte d'identité.

Une demande d'accès traitée en un mois



Article 12 du RGPD : un mois à compter de la réception, prolongeable de deux mois si la demande est complexe, en prévenant la personne dans le premier mois.

Le plus long est de tout retrouver. Cherchez dans les dossiers et la messagerie, mais aussi dans les conversations de l'outil d'IA, les fichiers joints, les fichiers enregistrés à part dans l'outil, sa mémoire, et ce que garde le sous-traitant. Avec une offre professionnelle, l'administrateur dispose en général d'outils d'export ou de recherche ; avec un compte personnel de salarié, vous ne pouvez rien chercher, ce qui suffit à exclure ces comptes du travail. C'est ici que paient les réglages de conservation de la leçon

« Choisir une offre d'IA selon l'entraînement, la conservation, le contrat et l'hébergement » et la ligne de « Inscrire un usage de l'IA au registre et informer les personnes concernées » : la ligne du registre donne d'un coup les finalités, les destinataires et la durée que l'article 15 vous demande d'indiquer.

Demande à recopier **Rédiger l'accusé de réception puis la réponse à une demande d'accès**

```
Rôle : tu aides une PME de [secteur] à répondre à une demande d'accès au titre de
l'article 15 du RGPD, en langage clair.
Contexte : demande reçue le [date] de [Personne A], [qualité : candidat, client,
salarié]. Ce que nous avons trouvé, sans donnée réelle : [catégories de données et
lieux : dossier, messagerie, conversations de l'outil d'IA]. Ligne du registre :
finalité [finalité] ; destinataires [services internes, éditeur de l'outil d'IA en tant
que sous-traitant] ; durée de conservation [durée] ; origine [source] ; décision
automatisée : [aucune / description].
Tâche 1 : écris l'accusé de réception, qui indique la date de réception et le délai
d'un mois.
Tâche 2 : écris la réponse qui donne, rubrique par rubrique, les informations de
l'article 15 et annonce la copie jointe des données.
Format : vouvoiement, phrases courtes, aucune information que je n'ai pas donnée,
crochets laissés là où il manque une information.
```

Ce que vous devez obtenir : Un accusé de réception de cinq lignes, puis une réponse en sept rubriques : confirmation du traitement, finalités, catégories de données, destinataires dont l'éditeur de l'outil d'IA, durée de conservation, origine des données, existence ou non d'une décision automatisée. La copie des données se prépare à part, depuis vos fichiers, jamais en recollant le dossier dans l'IA.

Note : Le modèle se remplit sans le nom ni les données de la personne : ils restent dans votre réponse finale, pas dans la demande à l'IA.

Quand une IA a lu ou décidé

« Une IA a-t-elle lu mon CV ? » appelle une réponse franche. Si un outil a résumé la candidature, dites-le : l'éditeur figure parmi les destinataires, et la personne doit savoir si une décision automatisée a été prise, avec la logique sous-jacente, dans ce cas (article 15). Si une décision fondée exclusivement sur un traitement automatisé l'a affectée significativement, l'article 22 lui ouvre le droit d'obtenir une intervention humaine, d'exprimer son point de vue et de contester la décision. Pour un système à haut risque de l'annexe III, comme le tri de candidatures, le règlement européen sur l'intelligence artificielle (AI Act) ajoute à partir du 2/12/2027 l'obligation d'informer les personnes visées par une décision qu'il aide à prendre (article 26, paragraphe 11). Un cabinet qui a suivi les leçons précédentes répond simplement : un outil a aidé à lire, une personne a décidé.

Ce qui est une violation de données

L'article 4, point 12, définit la violation comme une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles, ou l'accès non autorisé à ces données. Avec l'IA, quatre cas reviennent : un dossier de salarié ou de client collé dans un **compte gratuit**, chez un éditeur sans contrat de sous-traitance ; un **lien de partage public** d'une conversation qui contient des données ; un **connecteur** qui ouvre à un outil une boîte de messagerie entière ou un dossier partagé sans raison ; une **fuite chez l'éditeur** lui-même, qui doit alors vous prévenir dans les meilleurs délais (article 33, paragraphe 2). Toute violation se

documente dans le registre interne des violations (article 33, paragraphe 5), même celle qui ne se notifie pas.

Cinq incidents d'IA courants

Incident	Notifier la CNIL	Informer les personnes	Pourquoi
Un tableau de 40 salaires nominatifs collé dans un compte gratuit	Oui, sauf risque improbable démontré	À évaluer : oui si IBAN ou données de santé	Divulgation à un tiers sans contrat ; données financières
Lien de partage public d'une conversation avec des arrêts maladie, ouvert depuis l'extérieur	Oui	Oui, sans retard	Données de santé consultées sans droit : risque élevé
Lien public révoqué dans l'heure, jamais ouvert selon les éléments disponibles	Non, si le risque est improbable et documenté	Non	Accès refermé avant toute consultation
Connecteur ouvrant toute la boîte de la comptabilité à un outil sous contrat, sans fuite constatée	En général non	Non	Destinataire sous contrat ; le connecteur est restreint, l'incident documenté
Ordinateur portable volé, disque chiffré, conversations synchronisées	Selon l'évaluation	Non (article 34, paragraphe 3, a)	Données inintelligibles pour le voleur

Faut-il notifier la CNIL, faut-il informer les personnes

1 **L'incident est-il confiné : lien révoqué, accès coupé, éléments consignés ?**

Non — Confiner d'abord, dans les premières heures.

2 **Le risque pour les personnes est-il improbable, par exemple des données chiffrées ou un accès refermé sans consultation ?**

Non

Notifier la CNIL dans les 72 heures ; si le risque est élevé, informer aussi les personnes sans retard.

3 **L'entreprise est-elle responsable du traitement, et non sous-traitante de son client ?**

Non

Prévenir le client responsable dans les meilleurs délais ; c'est lui qui notifie, avec votre aide.

Oui à tout — **Documenter la violation dans le registre interne, sans notification.**

Dans tous les cas, la violation est documentée dans le registre interne (article 33, paragraphe 5). En cas de doute, la CNIL conseille de notifier.

Les 72 heures, heure par heure

Les 72 heures d'une violation

H0	H+4	H+24	H+72	J+3
Découverte	**Confinement**	**Évaluation**	**Notification**	**Information des personnes**
Heure notée, référent prévenu, rien de supprimé sans trace.	Lien révoqué, accès coupé, connecteur retiré, éléments consignés.	Quelles données, combien de personnes, quel risque.	Téléservice de la CNIL si le risque n'est pas improbable.	Sans retard si le risque est élevé, en langage clair.

Le délai court à partir du moment où l'entreprise a connaissance de la violation, pas à partir de l'incident.

L'article 33 demande de notifier la CNIL dans les meilleurs délais et, si possible, **72 heures au plus tard après en avoir pris connaissance**, sauf si la violation n'est pas susceptible d'engendrer un risque pour les personnes ; au-delà, la notification donne les motifs du retard. Elle se fait uniquement sur le téléservice de la CNIL, notifications.cnil.fr, et peut se faire en deux temps : une notification initiale dans le délai, puis une notification complémentaire quand l'enquête avance. L'article 34 ajoute l'information des personnes, dans les meilleurs délais, quand le risque est élevé, sauf données chiffrées, risque écarté par des mesures prises ensuite, ou effort disproportionné, remplacé alors par une communication publique. Une réforme est en discussion à Bruxelles ; tant qu'elle n'est pas adoptée, les règles de cette leçon s'appliquent.

Confiner un incident dans ChatGPT, relevé du 19/11/2026

1. Avant toute suppression, notez l'heure, le titre de la conversation, ce qu'elle contient et le nombre de personnes concernées, ou faites une capture conservée par le référent.
2. Pour un lien partagé : ouvrez Paramètres, puis Commandes des données (Data controls), puis Gérer en face de Liens partagés (Shared links).
3. Choisissez « Supprimer le lien partagé » pour le lien concerné. Le lien ne s'ouvre plus ; la conversation d'origine reste, et les copies déjà enregistrées par d'autres ne sont pas effacées.
4. Pour la conversation : dans l'historique, ouvrez le menu ••• de la conversation, choisissez Supprimer et confirmez. Elle disparaît tout de suite de l'affichage et est supprimée des systèmes de l'éditeur sous 30 jours, sauf obligation de sécurité ou légale, selon sa page d'aide.
5. Supprimer la conversation supprime aussi son lien partagé, mais pas les fichiers enregistrés à part dans la bibliothèque de l'outil : supprimez-les séparément.
6. Les libellés peuvent varier selon la version et la langue de l'interface. Pour un connecteur trop large, déconnectez-le depuis les réglages des applications ou connecteurs de l'outil, puis retirez l'autorisation côté messagerie.

Demande à recopier **Préparer la fiche de la violation et la trame de notification**

```
Rôle : tu aides le référent d'une PME de [effectif] personnes à documenter une
violation de données, sans avis juridique.
Contexte, sans aucune donnée réelle : découverte le [date] à [heure] par [fonction]. Ce
qui s'est passé : [faits]. Données touchées : [catégories]. Nombre approximatif de
personnes : [nombre]. Mesures déjà prises : [liste avec heures]. Responsable du
traitement : [nous / notre client].
Tâche 1 : rédige la fiche du registre interne des violations : faits, effets, mesures,
décision de notifier ou non et sa justification.
Tâche 2 : rédige la trame de notification qui reprend les quatre éléments de l'article
33, paragraphe 3 : nature de la violation (catégories et nombre approximatif de
personnes et d'enregistrements), contact, conséquences probables, mesures prises ou
proposées.
Format : deux blocs titrés, phrases courtes, crochets là où il manque une information.
N'évalue pas toi-même le risque : liste les éléments qui permettent de l'évaluer.
```

Ce que vous devez obtenir : Une fiche d'une demi-page datée et une trame en quatre rubriques, prête à reporter sur le téléservice. Les crochets restants sont la liste de ce que l'enquête doit encore établir avant la notification complémentaire.

Demande à recopier **Rédiger le message aux personnes concernées**

```
Rôle : tu rédiges un message d'information après une violation de données, en langage
clair, pour des personnes qui ne connaissent pas le RGPD.
Contexte : [ce qui s'est passé, en deux phrases] ; données touchées : [catégories] ;
date : [date] ; mesures prises : [liste] ; ce que les personnes peuvent faire :
[vigilance précise, par exemple sur les courriels qui demandent des coordonnées
bancaires] ; contact : [prénom, fonction, téléphone, adresse électronique].
Tâche : écris le message.
Format : dix lignes au plus, vouvoiement, un objet clair. Il décrit la nature de la
violation, le contact, les conséquences probables et les mesures prises. Aucune formule
qui minimise, aucune promesse que nous ne pouvons pas tenir.
```

Ce que vous devez obtenir : Un message daté qui commence par les faits, nomme les données touchées, dit ce que l'entreprise a fait et ce que la personne peut faire, puis donne un contact direct. L'article 34 demande des termes clairs et simples : relisez-le comme la personne qui le recevra un vendredi soir.

Ce que l'erreur coûte

Les plafonds de l'article 83 vont jusqu'à 20 M€ ou 4 % du chiffre d'affaires annuel mondial pour les principes et les droits des personnes (articles 5 à 9, 12 à 22, transferts), et jusqu'à 10 M€ ou 2 % pour les obligations du responsable et du sous-traitant, dont la sécurité et la notification (articles 25 à 39), le montant le plus élevé étant retenu. Les sanctions de 2026 donnent la mesure : Free Mobile et Free, 42 M€ au total le 8/1/2026 ; France Travail, 5 M€ le 22/1/2026 pour la sécurité des données des demandeurs d'emploi ; une société sanctionnée de 5 M€ annoncée le 18/11/2026 pour des mots de passe de clients conservés en clair ; et 38 sanctions en procédure simplifiée annoncées le 17/11/2026, qui touchent aussi de petites structures. **Aucune ne porte sur l'IA** : toutes portent sur la sécurité, l'information des personnes ou la conservation, exactement les règles qu'un usage de l'IA met à l'épreuve.

La sanction de Free Mobile et Free

Délibérations SAN-2026-001 et SAN-2026-002 du 8/1/2026 : 27 M€ pour Free Mobile, 15 M€ pour Free. Environ 24 millions de contrats d'abonnés touchés, IBAN compris pour une partie des clients. Manquements à l'article 32 (sécurité) et à l'article 34 (information incomplète des personnes) pour les deux sociétés, et à l'article 5-1-e (conservation excessive) pour Free Mobile, avec des injonctions à trois et six mois. Source : CNIL, relevé du 19/11/2026.

Notre position

Écrivez la procédure « droits et fuite » sur une page et affichez-la avant d'en avoir besoin : qui reçoit les demandes, où chercher, qui décide de notifier, l'adresse du téléservice. Le jour de l'incident, personne ne lit une procédure de dix pages. Et un salarié qui signale son erreur dans l'heure mérite des remerciements : c'est lui qui vous donne vos 72 heures.

Les erreurs fréquentes

L'erreur, et pourquoi elle coûte	La correction
Supprimer la conversation fautive dans la minute, sans rien noter. Vous ne pouvez plus dire quelles données sont parties ni combien de personnes sont touchées, alors que la documentation et la notification le demandent.	Consignez d'abord l'heure, le contenu et le nombre de personnes, ou faites une capture conservée par le référent, puis supprimez le lien et la conversation.
Attendre d'avoir tout compris pour notifier la CNIL. Les 72 heures courent depuis la prise de connaissance, week-end compris. Une enquête complète dépasse souvent ce délai.	Faites une notification initiale dans le délai avec ce que vous savez, puis une notification complémentaire quand l'enquête avance, comme le téléservice le permet.
Répondre à une demande d'accès avec le seul dossier principal. Les conversations d'IA, les fichiers joints et ce que garde le sous-traitant sont aussi des données de la personne. Une réponse incomplète méconnaît l'article 15.	Partez de la ligne du registre : chaque destinataire et chaque outil cités sont un endroit où chercher, outil d'IA compris.
Exiger une copie de pièce d'identité avant de répondre à toute demande. L'article 12 ne permet de demander des informations supplémentaires qu'en cas de doute raisonnable sur l'identité. Exiger une pièce sans raison collecte une donnée de plus et retarde la réponse.	Répondez à l'adresse connue de la personne ; ne demandez un élément supplémentaire que si un doute réel existe, et seulement ce qui suffit à le lever.

Exercice : Une conversation partagée par erreur à l'usine de Bègles

Lundi 16 novembre, 9 h 10, Isabelle, DRH de l'usine de Bègles (85 salariés), apprend par un salarié qu'un lien de partage public d'une conversation circule dans un groupe de messagerie de l'atelier. Un chef d'équipe y avait demandé à un outil d'IA sous contrat de « préparer le planning de

décembre » en collant la liste des 23 opérateurs de son équipe, avec leurs absences du mois et le motif de chacune (dont quatre arrêts maladie et un congé maternité). Le lien a été créé jeudi dernier ; le salarié l'a ouvert dimanche. Établissez la conduite à tenir de 9 h 10 à jeudi 9 h 10.

1. Listez les gestes de la première heure, dans l'ordre.
2. Passez l'incident dans l'arbre « Faut-il notifier la CNIL, faut-il informer les personnes » et justifiez chaque réponse.
3. Remplissez la trame de notification en quatre rubriques.
4. Rédigez le message aux 23 opérateurs.
5. Dites ce qui change dans la charte et dans la fiche de l'usage.

Le corrigé est dans le cahier d'exercices et sur la page de la leçon.

À retenir

- Une demande de droits reçoit une réponse dans un délai d'un mois, gratuite, prolongeable de deux mois en prévenant la personne dans le premier mois.
- La recherche couvre les conversations d'IA, les fichiers envoyés, la mémoire de l'outil et ce que garde le sous-traitant.
- Toute violation se documente ; elle se notifie à la CNIL sous 72 heures si le risque n'est pas improbable, et s'annonce aux personnes s'il est élevé.
- Le délai court à partir du moment où l'entreprise sait ; un sous-traitant prévient son client responsable dans les meilleurs délais.
- Avant de supprimer une conversation ou un lien, consignez ce qu'ils contenaient : c'est ce qui permet d'évaluer le risque.

Leçon 8 | 42 min | Accès libre

Votre plan sur 30 jours et l'évaluation finale

> Le cours se termine par un plan de quatre semaines pour mettre votre entreprise en règle : inventaire des outils et des comptes, choix des offres et contrats, registre, mentions et rangement AI Act, puis charte, formation et procédure « droits et fuite ». L'évaluation finale compte 40 questions sur les trois modules et une épreuve pratique de 60 minutes notée sur 20.

Objectifs

- Établir un plan de 30 jours qui mène de l'inventaire des usages réels à une charte présentée et une procédure affichée
- Choisir l'ordre des actions selon le risque pour les personnes et l'effort demandé
- Valider le cours par l'évaluation finale en 40 questions et l'épreuve pratique de 60 minutes

Le cours

Un cours sur le RGPD et l'IA ne vaut que par ce qui change chez vous un mois plus tard. Cette dernière leçon transforme les sept leçons précédentes en un plan de quatre semaines, à raison de deux à trois heures par semaine, autour de la question qui a guidé tout le cours : **qu'est-ce qui part, chez qui, pour quoi faire, et qui le sait ?** Elle se termine par l'évaluation finale : 40 questions de mise en situation, puis une épreuve pratique de 60 minutes sur le dossier complet d'une PME.

Vos 30 jours

Semaine 1	Semaine 2	Semaine 3	Semaine 4	Jour 30
Inventaire	**Offres et contrats**	**Registre et AI Act**	**Charte et procédure**	**Prochaine relecture**
Outils et comptes réellement utilisés, comptes personnels compris, et données qui y passent.	Offres choisies, réglages faits, contrats signés, comptes gratuits fermés pour le travail.	Lignes du registre, mentions d'information à jour, usages rangés selon l'AI Act.	Charte présentée, formation datée, procédure « droits et fuite » affichée.	Date inscrite à l'agenda, dans six mois au plus tard.

Deux à trois heures par semaine suffisent dans une PME de moins de 50 personnes ; chaque semaine laisse une preuve datée.

Semaine 1, l'inventaire des usages réels

Listez chaque outil d'IA utilisé dans l'entreprise, avec l'offre, le titulaire du compte et les données qui y passent. L'inventaire compte les comptes personnels : dans la plupart des PME, ce sont eux qui portent le risque. Le plus fiable est un questionnaire anonyme de cinq questions, envoyé à toute l'équipe avec la promesse écrite qu'aucune réponse ne sera reprochée. Rangez ensuite chaque usage avec la grille de « Ce qui devient une donnée personnelle quand vous écrivez à une IA » : aucune donnée, données personnelles, données sensibles.

Le tableau d'inventaire à recopier

Usage (verbe + objet)	Outil et offre	Compte	Données qui partent	Mesure actuelle	Décision
[usage]	[outil, gratuit ou professionnel]	[entreprise ou personnel]	[aucune, personnelles, sensibles]	[aucune, pseudonymisation, colonnes retirées]	[garder, régulariser, fermer]
Rédiger les briefs créatifs	Assistant, offre gratuite	Personnel, 3 salariés	Noms et budgets de clients	Aucune	Fermer, passer à l'offre de l'agence
Résumer les verbatims d'enquête	Assistant, offre professionnelle	Entreprise	Verbatims	Noms remplacés par [Répondant n]	Garder

Demande à recopier **Préparer le questionnaire anonyme de la semaine 1**

```
Rôle : tu aides la direction d'une PME de [effectif] personnes, secteur [secteur], à
recenser les usages réels de l'IA.
```

```
Tâche : rédige un questionnaire anonyme de cinq questions à envoyer à toute l'équipe :
quels outils d'IA vous utilisez pour le travail ; avec quel compte (de l'entreprise,
personnel gratuit, personnel payant) ; pour quelles tâches ; quel type d'informations
vous y mettez (aucune donnée sur des personnes, coordonnées, données de clients ou de
salariés, santé ou données bancaires) ; ce qui vous manque pour travailler avec les
outils de l'entreprise.
Format : un message d'introduction de trois lignes qui promet qu'aucune réponse ne sera
reprochée, puis les cinq questions à choix multiples avec une case « autre ».
```

Ce que vous devez obtenir : Un questionnaire prêt à coller dans un formulaire en ligne de l'entreprise, sans question qui permette d'identifier la personne qui répond. Le résultat donne l'inventaire réel, comptes personnels compris.

Semaine 2, offres, réglages et contrats

Pour chaque outil gardé, posez les cinq questions de « Choisir une offre d'IA selon l'entraînement, la conservation, le contrat et l'hébergement » : entraînement, conservation, contrat de sous-traitance de l'article 28, hébergement, transferts hors de l'Union. Signez ou téléchargez le contrat, faites les réglages, notez la date du relevé des conditions. Puis fermez pour le travail les comptes gratuits personnels, en donnant à chacun un accès à l'offre de l'entreprise le jour même : une fermeture sans solution renvoie l'usage dans l'ombre.

Le sort de chaque compte après la semaine 2

Garder

- Offre professionnelle sous contrat de sous-traitance
- Entraînement exclu, conservation réglée
- Outil inscrit au registre

Régulariser dans la semaine

- Offre payante sans contrat signé
- Réglages non vérifiés depuis le dernier relevé
- Connecteur ouvert sans besoin écrit

Fermer pour le travail

- Compte personnel gratuit d'un salarié
- Outil inconnu de la direction
- Outil qui refuse tout contrat de sous-traitance

Un compte reste orange une semaine au plus : il passe au vert ou il ferme.

Semaine 3, registre, mentions et AI Act

Un usage de l'IA modifie le plus souvent un traitement existant : la ligne du recrutement ou de la gestion des clients s'enrichit d'un destinataire, l'éditeur sous-traitant, d'un pays et d'une mesure. Complétez ces lignes, puis mettez à jour les mentions d'information concernées : offre d'emploi, formulaire de contact, politique de confidentialité, lettre de mission. Ajoutez enfin une colonne « niveau AI Act », pour le règlement européen sur l'intelligence artificielle, rangée avec l'arbre de « Ce que l'AI Act demande à une PME qui utilise l'IA, de la formation au recrutement ». Tout usage qui touche un candidat, un salarié ou le crédit d'un particulier passe en tête de la liste des corrections.

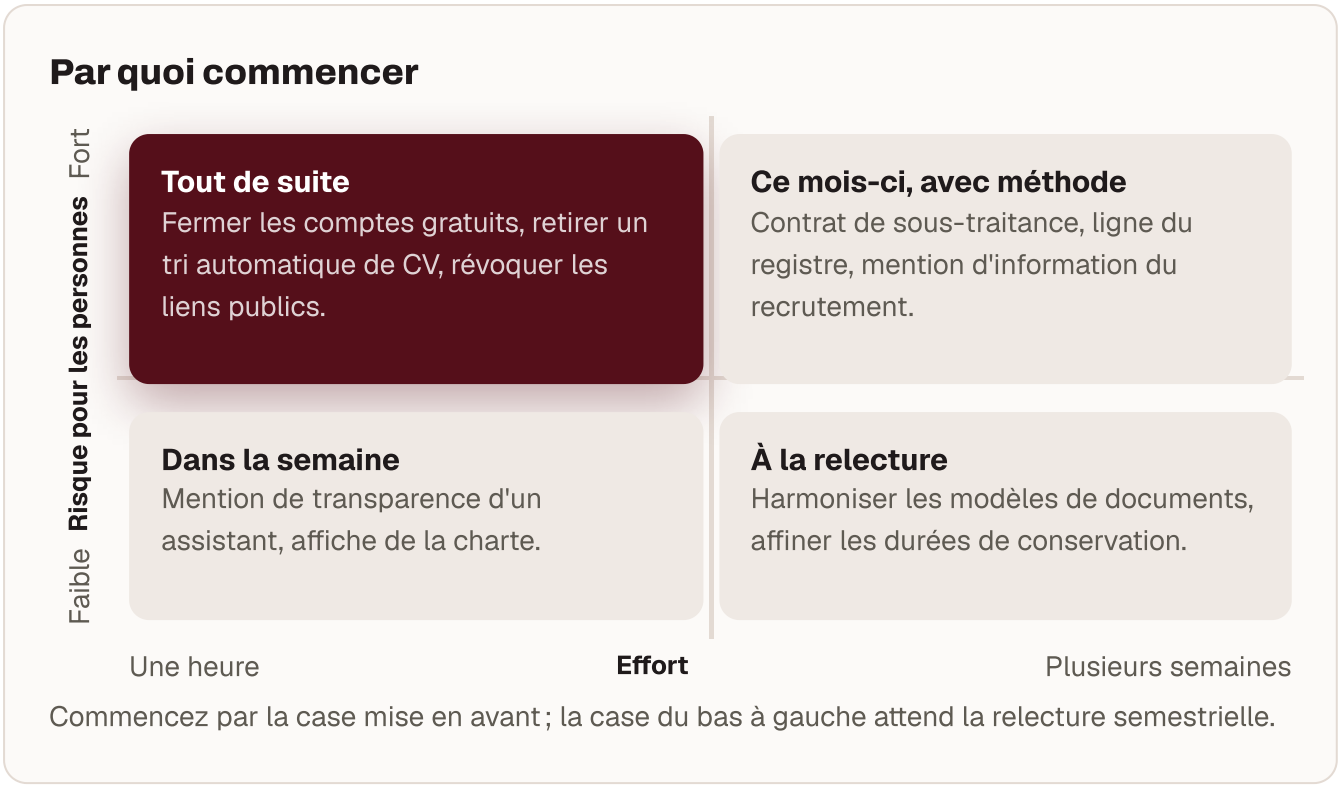
Demande à recopier **Rédiger les lignes du registre et la colonne AI Act**

```
Rôle : tu aides une PME à tenir son registre des traitements, sans avis juridique.
Contexte : voici notre inventaire, sans aucune donnée personnelle : [collez le tableau
de la semaine 1, colonnes usage, outil et offre, données qui partent, mesure]. Pour
chaque outil : contrat de sous-traitance signé le [date], hébergement [lieu], transfert
hors Union [oui ou non, fondement].
Tâche : pour chaque usage, propose la ligne du registre (finalité, catégories de
personnes et de données, destinataires dont l'éditeur en tant que sous-traitant,
transfert et fondement, durée de conservation, mesures de sécurité) et un niveau AI Act
(pratique interdite, haut risque, transparence, risque minimal) avec le critère qui le
justifie.
Format : un tableau, puis une liste « À faire examiner » pour tout point qui dépend
d'une information absente. N'invente aucune durée : laisse [durée] quand je ne l'ai pas
donnée.
```

Ce que vous devez obtenir : Un tableau d'une ligne par usage, avec des crochets là où une décision vous revient, et trois à cinq points « À faire examiner ». Chaque ligne se relit avec la fiche de l'usage avant d'entrer au registre.

Semaine 4, charte, formation et procédure

Rédigez la charte en sept parties avec la méthode de « Écrire la charte d'usage de l'IA de l'entreprise et la faire vivre », suivez la procédure qui convient à votre effectif, présentez-la en 30 minutes et datez chaque formation. Affichez à côté la procédure « droits et fuite » de « Répondre à une demande d'exercice de droits et réagir à une fuite de données » : qui reçoit les demandes, où chercher, qui décide de notifier, l'adresse du téléservice de la Commission nationale de l'informatique et des libertés (CNIL). Le jour 30, inscrivez à l'agenda la prochaine relecture, dans six mois au plus tard.



L'évaluation finale

L'évaluation compte **40 questions de mise en situation** : 13 sur le module 1 (les données que vous confiez à une IA), 13 sur le module 2 (choisir ses outils et tenir ses obligations), 14 sur le module 3 (l'AI Act, la charte et les incidents). Chaque question n'a qu'une bonne réponse, corrigée automatiquement ; aucune ne porte sur un libellé d'interface. Vient ensuite l'épreuve pratique, le dernier entraînement de la leçon : 60 minutes sur le dossier d'un négoce de matériaux, notées sur 20 avec la grille ci-dessous. Un formateur de Bonbay Académie répond à vos questions sous 24 heures ouvrées ; décrivez la situation, sans y mettre de données personnelles réelles.

La grille de l'épreuve pratique sur 20 points

Partie	Points	Ce qui donne les points
Éliminatoire	Épreuve à refaire	Une donnée identifiante laissée dans le texte destiné à l'IA, un tri automatique de candidatures accepté, ou un incident non documenté
Texte pseudonymisé	4	Identifiants directs retirés, étiquettes stables et table hors de l'IA, généralisation utile, donnée de santé retirée
Choix de l'offre	4	Offre retenue, entraînement et contrat de sous-traitance, transfert et son fondement, conservation et registre
Registre et mention	4	Rubriques de la ligne, éditeur sous-traitant, mention claire avec destinataire, transfert, durée et droits
Rangement AI Act	4	Un point par usage bien rangé, un point pour les mesures de l'article 4
Incident	4	Consigner puis confiner, documenter, décider de notifier avec l'échéance, décider d'informer et corriger la charte

Ce qu'il faut viser

Visez 32 bonnes réponses sur 40 et 16 sur 20 à l'épreuve, sans critère éliminatoire. Une partie de l'épreuve à moins de la moitié de ses points désigne la leçon à reprendre : le texte pseudonymisé renvoie à « Anonymiser ou pseudonymiser une demande et un fichier avant de les envoyer », le choix de l'offre à « Choisir une offre d'IA selon l'entraînement, la conservation, le contrat et l'hébergement », le registre à « Inscrire un usage de l'IA au registre et informer les personnes concernées », le rangement à « Ce que l'AI Act demande à une PME qui utilise l'IA, de la formation au recrutement », l'incident à « Répondre à une demande d'exercice de droits et réagir à une fuite de données ».

Les erreurs fréquentes

L'erreur, et pourquoi elle coûte	La correction
Commencer par rédiger la charte, avant tout inventaire. La charte parle alors d'outils et de données théoriques. Elle ignore les comptes personnels et les usages réels, qui portent le risque.	Faites l'inventaire en semaine 1, avec un questionnaire anonyme, et écrivez la charte en semaine 4 à partir de ce que l'équipe fait vraiment.
Fermer les comptes gratuits des salariés sans leur donner d'outil de remplacement. Le besoin reste, et l'usage repart sur les téléphones personnels, hors de vue. Le risque est déplacé, pas réduit.	Ouvrez l'accès à l'offre professionnelle de l'entreprise le jour même de la fermeture, et annoncez-le dans le même message.
Tout faire sans rien dater. L'article 4 de l'AI Act et la responsabilité du RGPD demandent de pouvoir montrer les mesures prises. Sans date, une formation ou une relecture n'existe pas aux yeux d'un contrôleur ou d'un client.	Chaque semaine laisse une preuve datée : inventaire, contrats et relevés des conditions, registre, charte, accusés de lecture, registre des formations.
Considérer que tout est réglé au jour 30. Les outils, leurs conditions et les usages de l'équipe changent en quelques mois. Un registre et une charte jamais relus décrivent vite une entreprise qui n'existe plus.	Inscrivez la prochaine relecture à l'agenda, dans six mois au plus tard, et relisez à chaque nouvel outil.

Exercice : Votre plan sur 30 jours

Écrivez votre propre plan sur 30 jours, à partir de votre entreprise. Si vous préférez vous exercer d'abord, faites-le pour l'usine de Bègles (85 salariés, pièces en aluminium). Isabelle, DRH, a relevé : Microsoft 365 Copilot payé pour 12 cadres ; trois techniciens du bureau d'études qui utilisent un assistant gratuit personnel pour traduire des cahiers des charges de clients ; un projet de logiciel de recrutement avec score automatique pour 30 embauches en 2027 ; un fournisseur qui propose une caméra « d'humeur » ; aucune charte, un registre sans ligne sur l'IA, un CSE qui se réunit le premier mardi du mois.

1. Semaine 1 : dressez l'inventaire et classez les données qui passent dans chaque outil.
2. Semaine 2 : décidez du sort de chaque compte et des contrats à signer.

3. Semaine 3 : listez les lignes du registre, les mentions à mettre à jour et le niveau AI Act de chaque usage.
4. Semaine 4 : prévoyez la charte, sa procédure, la formation, la procédure « droits et fuite » et la date de relecture.

Le corrigé est dans le cahier d'exercices et sur la page de la leçon.

À retenir

- Semaine 1, l'inventaire réel, comptes personnels compris ; semaine 2, offres, contrats et comptes gratuits fermés pour le travail.
- Semaine 3, registre, mentions et rangement AI Act ; semaine 4, charte, formation datée et procédure « droits et fuite » affichée.
- Commencez par ce qui protège le plus pour le moins d'effort : comptes gratuits, tri automatique de CV, liens publics, pratiques interdites.
- Chaque semaine laisse une preuve datée ; le jour 30, la prochaine relecture est inscrite à l'agenda.