Projet à valider avant diffusion. Ce bandeau, l'annexe 2 et la note de transmission en fin de document sont à supprimer une fois la charte relue par votre conseil et adoptée selon la clause « Opposabilité ».

Charte d'usage de l'intelligence artificielle

[Raison sociale]
Version 1 du [date de la version]
Entrée en vigueur : [date d'entrée en vigueur]
Référent IA : [Référent IA à désigner]

L'essentiel

- J'utilise les outils validés ([liste des outils validés, à compléter avant diffusion]) avec le compte fourni par l'entreprise.
- Je ne saisis jamais de mot de passe, de clé d'accès, de numéro de sécurité sociale ni de coordonnées bancaires. Je garde hors de ces outils les données personnelles de clients, de salariés ou de candidats et les secrets d'affaires, sauf environnement contractualisé validé par [Référent IA à désigner].
- Je vérifie tout résultat avant de l'utiliser : j'en réponds comme de mon propre travail.
- Je signale sans délai, et au plus tard le jour même, toute erreur ou fuite à [Référent IA à désigner]. Le fait de signaler de bonne foi n'est jamais sanctionné, et une erreur involontaire signalée n'est pas une faute.
- Je suis la formation avant d'utiliser les outils.

Le détail et les sources suivent.

1. Objet

La présente charte fixe les règles d'utilisation des systèmes d'intelligence artificielle par les personnes travaillant pour [Raison sociale]. Elle vise un usage utile et maîtrisé de ces outils, la protection des données confiées à l'entreprise et le respect du règlement (UE) 2024/1689 sur l'intelligence artificielle ainsi que du règlement général sur la protection des données.

2. Champ d'application

Elle s'applique aux salariés, stagiaires, alternants et prestataires intervenant pour [Raison sociale], quel que soit le matériel utilisé, y compris les équipements personnels et les usages en télétravail.

3. Statut au regard du règlement sur l'IA

En clair : en utilisant des outils d'IA conçus par d'autres, [Raison sociale] en est « déployeur » ; en créant un outil d'IA proposé sous son nom, elle en deviendrait « fournisseur », avec des obligations plus lourdes.

Le détail suit.

Lorsque l'organisation utilise sous sa propre autorité les outils listés dans la présente charte, [Raison sociale] est un déployeur au sens de l'article 3, point 4, du règlement (UE) 2024/1689. L'organisation devient fournisseur si elle développe ou fait développer un système d'IA et le met en service sous son propre nom, par exemple un assistant conversationnel destiné à ses clients (article 3, point 3). Elle peut aussi être considérée comme fournisseur d'un système à haut risque si elle modifie la destination d'un outil, y compris un outil d'IA à usage général, de sorte qu'il relève de l'annexe III, par exemple pour trier des candidatures (article 25, paragraphe 1, point c). Tout projet de ce type est soumis à [Référent IA à désigner] avant son lancement et fait l'objet d'une analyse juridique.

4. Principes directeurs

Cinq principes guident l'usage de l'IA chez [Raison sociale]. Ils s'inspirent de la charte éthique de la Cour de cassation et constituent des principes d'organisation, non des obligations légales propres aux entreprises privées.

- **L'IA assiste, elle ne décide pas.** Aucune décision individuelle (recrutement, évaluation, sanction, accès à un droit) n'est prise sur la seule base d'un résultat produit par une IA.
- **La personne qui reprend un contenu en répond.** Reprendre, même partiellement, un contenu généré par une IA, c'est en répondre comme de son propre travail. L'erreur ne peut être imputée à l'outil.
- **Réfléchir avant de solliciter l'IA.** Lorsque l'IA sert à préparer une décision ou un travail, la personne conduit d'abord sa propre réflexion, puis consulte le résultat, afin de limiter le biais d'ancrage. Elle garde un esprit critique pendant tout l'échange.
- **Préserver et transmettre les savoir-faire.** Avant d'ouvrir l'IA à une personne nouvellement arrivée, l'entreprise s'assure qu'elle sait réaliser sans aide les tâches qui lui sont confiées, puis la forme aux outils validés.
- **Sobriété.** Avant de recourir à l'IA, on se demande si un moyen plus simple et plus frugal donne le même résultat. Si oui, il est préféré.

Source : Cour de cassation, Charte éthique relative à l'utilisation des systèmes d'intelligence artificielle, arrêtée au 30 septembre 2026, principes 1 (prééminence humaine), 2 (maîtrise humaine) et 3 (responsabilité humaine).

5. Outils autorisés et comptes utilisés

Les outils validés à ce jour, utilisés avec un compte fourni par l'entreprise et inscrits au registre des outils, sont : [liste des outils validés, à compléter avant diffusion]. Tout autre outil est soumis à l'accord préalable de [Référent IA à désigner] et inscrit au registre des outils avant son premier usage professionnel.

L'usage professionnel passe par les comptes fournis par l'entreprise. L'utilisation d'un compte personnel, d'une version gratuite non validée ou d'une extension de navigateur installée à titre individuel est proscrite : l'entreprise perd alors toute maîtrise sur les données saisies et sur leur réutilisation éventuelle pour l'entraînement des modèles.

6. Données interdites en saisie

Ne sont jamais saisis dans un outil d'IA, même validé : les mots de passe, codes d'accès, clés d'API et autres secrets d'authentification ; le numéro de sécurité sociale, les numéros de pièces d'identité et les coordonnées bancaires complètes ; les données de santé et les autres catégories particulières de données (origine, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques ou biométriques, vie sexuelle ou orientation sexuelle, article 9 du RGPD), ainsi que les données relatives aux condamnations pénales et aux infractions (article 10) ; les signalements et les éléments d'une enquête interne qui permettent d'identifier leur auteur, les personnes visées ou les témoins ; les consultations et correspondances d'avocat et les pièces d'un contentieux, sauf accord préalable de la direction.

Il est interdit de saisir dans un outil d'IA, hors environnement contractualisé validé par [Référent IA à désigner] : données personnelles de clients, de salariés ou de candidats, ainsi que tout secret d'affaires et tout élément couvert par une clause de confidentialité. Les environnements contractualisés sont signalés comme tels au registre des outils : un outil validé n'en fait pas partie s'il n'y est pas signalé. Seules les données nécessaires à la tâche sont saisies, et les noms, coordonnées et références de dossier sont retirés ou remplacés lorsque la tâche le permet : une donnée ainsi pseudonymisée reste une donnée personnelle. En cas de doute sur une donnée, la règle est de ne pas la saisir et d'en parler à [Référent IA à désigner].

Niveau	Données	Où les utiliser
Jamais	Mots de passe et clés d'accès ; numéro de sécurité sociale, pièces d'identité, coordonnées bancaires ; données de santé et autres données sensibles ; condamnations et infractions ; signalements et enquêtes internes ; correspondances d'avocat	Dans aucun outil d'IA
Sous conditions	Données personnelles de clients, de salariés ou de candidats, secrets d'affaires, informations reçues sous engagement de confidentialité	Uniquement dans un environnement contractualisé validé par [Référent IA à désigner]
Usage courant	Informations publiques, documents internes sans donnée personnelle ni information confidentielle	Dans tout outil listé à la clause « Outils autorisés et comptes utilisés »

Au moins un outil validé héberge ou traite les données en dehors de l'Union européenne, ou peut y donner accès. Ces transferts relèvent du chapitre V du RGPD. La mention du lieu d'hébergement, le cadre de transfert invoqué par l'éditeur et le contrat de sous-traitance prévu à l'article 28 du RGPD sont conservés, pour chaque outil, par [Référent IA à désigner]. Les traitements portant sur les catégories de données listées ci-dessus se font par priorité sur un outil hébergé dans l'Union.

La localisation des serveurs ne suffit pas : le pays d'établissement de l'éditeur, les entités qui opèrent le service et ses sous-traitants sont aussi vérifiés, car un service hébergé dans l'Union peut rester soumis à une législation étrangère. Les réglages par défaut (mémoire, recherche web, connecteurs, partage,

modèles d'autres éditeurs) sont revus à l'activation de chaque outil puis après chaque mise à jour importante, et la suppression des données est demandée par écrit à l'éditeur en fin de contrat.

7. Usages interdits

Aucun système d'IA n'est utilisé pour déduire les émotions d'un salarié ou d'un candidat. Lorsque cette déduction repose sur des données biométriques (visage, voix), elle est interdite sur le lieu de travail par l'article 5, paragraphe 1, point f, du règlement (UE) 2024/1689 depuis le 2 février 2025, hors raisons médicales ou de sécurité ; dans les autres cas, l'interdiction est une règle de l'entreprise. Est également interdite la catégorisation biométrique qui déduit l'origine raciale, les opinions politiques, l'affiliation syndicale, les convictions religieuses ou philosophiques, la vie sexuelle ou l'orientation sexuelle d'une personne (article 5, paragraphe 1, point g). À partir du 2 décembre 2026, il est également interdit d'utiliser un système d'IA dans le but de générer ou de manipuler des images, des vidéos ou des contenus audio réalistes représentant les parties intimes d'une personne identifiable, ou la montrant se livrant à des activités sexuellement explicites, sans son consentement libre, spécifique, éclairé, univoque et explicite, ainsi que tout contenu pédopornographique (article 5, paragraphe 1, points b bis et b ter, ajoutés par le règlement (UE) 2026/1744). Sont également interdites, depuis le 2 février 2025, la notation sociale des personnes qui conduit à un traitement préjudiciable sans rapport avec le contexte des données ou disproportionné (article 5, paragraphe 1, point c) et les techniques subliminales, manipulatrices ou trompeuses qui altèrent substantiellement le comportement d'une personne en lui causant un préjudice important (point a). Par décision de l'entreprise, toute notation sociale et tout usage destiné à manipuler un interlocuteur sont proscrits, même hors de ces conditions.

8. Vérification des résultats

Un résultat produit par une IA est un brouillon. La personne qui l'utilise en vérifie l'exactitude avant tout usage professionnel et en répond. Les chiffres, citations, références juridiques, coordonnées et sources sont contrôlés à la source. Cette règle ne met à la charge de personne les conséquences financières d'une erreur.

Un contenu reçu dont l'authenticité est douteuse (message vocal, vidéo, document, demande inhabituelle de paiement ou de transmission de données) est vérifié par un autre canal avant toute suite, même lorsque la voix ou l'image paraissent authentiques : une IA permet d'imiter l'une et l'autre.

9. Sécurité des comptes et des accès

Chaque compte est personnel : identifiants non partagés, mot de passe propre à chaque outil, authentification multifacteur activée lorsqu'elle est disponible. Aucun espace ni aucune conversation n'est partagé avec une personne extérieure sans l'accord de [Référent IA à désigner].

Un outil d'IA n'accède à la messagerie, aux espaces documentaires, aux agendas, au code source ou à une application métier qu'après validation de [Référent IA à désigner], avec les seuls droits nécessaires, revus régulièrement. Les extensions, connecteurs et assistants préconfigurés, y compris ceux partagés entre collègues, ne sont installés qu'après la même validation. Aucun outil n'exécute seul une action critique

(envoi vers l'extérieur, publication, paiement, modification ou suppression de données) sans validation humaine préalable de l'action ou de son paramétrage.

Un document, une page web ou un message reçu peut contenir des instructions cachées destinées à détourner l'outil qui le lit : on se méfie d'une réponse inattendue et aucun outil n'agit sur la base d'un contenu externe non vérifié.

10. Propriété intellectuelle

Les contenus produits avec l'aide d'une IA sont vérifiés avant diffusion : ils peuvent reproduire une œuvre existante, une marque ou un visuel protégé, et la protection par le droit d'auteur d'un contenu généré sans intervention humaine caractérisée reste incertaine. Les productions destinées à être protégées ou déposées comportent une part de création humaine documentée. Aucun contenu soumis à une licence restrictive, aucun code sous licence incompatible avec nos usages ne sont réutilisés sans vérification.

11. Données personnelles : registre, conservation, analyse d'impact

Chaque outil d'IA utilisé sur des données personnelles est inscrit au registre des traitements prévu à l'article 30 du RGPD, avec sa finalité, ses catégories de données, ses destinataires et sa durée de conservation. Les historiques de conversation constituent eux-mêmes un traitement : leur durée de conservation est fixée à [durée à compléter] et l'option d'entraînement des modèles sur nos contenus est désactivée lorsque l'éditeur la propose.

Une analyse d'impact relative à la protection des données, au sens de l'article 35 du RGPD, est conduite avant tout usage susceptible d'engendrer un risque élevé pour les personnes, en particulier ceux qui figurent sur la liste publiée par la CNIL, comme la surveillance constante de l'activité des salariés ou le profilage à des fins de gestion des ressources humaines, et ceux qui réunissent plusieurs critères retenus par le comité européen de la protection des données, comme l'évaluation ou la notation de personnes, la décision automatisée avec effet juridique ou le traitement de données sensibles à grande échelle.

Pour chaque usage portant sur des données personnelles, le registre indique la base légale retenue (article 6 du RGPD) et la façon dont les personnes concernées, clients, salariés ou candidats, en sont informées (articles 13 et 14). Si un délégué à la protection des données a été désigné, il est consulté avant la validation de tout outil et lors de toute analyse d'impact (articles 35, paragraphe 2, et 38, paragraphe 1).

12. Incident et violation de données

Tout incident (donnée confidentielle saisie par erreur, fuite, comportement inattendu d'un outil ou d'un agent, accès non autorisé) est signalé à [Référent IA à désigner] sans délai, et au plus tard le jour même. Lorsque l'incident constitue une violation de données personnelles, le risque est apprécié par [Référent IA à désigner] et la violation est, le cas échéant, notifiée à la CNIL dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance (article 33 du RGPD), les personnes concernées étant informées dans les conditions de l'article 34. Chaque violation est consignée dans le registre interne des violations, qu'elle soit notifiée ou pas.

13. Prestataires et intervenants extérieurs

Les prestataires qui interviennent sur nos dossiers appliquent la présente charte. Ils s'engagent à ne pas saisir nos données dans un outil d'IA qui ne figure pas à la liste des outils validés, sauf accord écrit de [Référent IA à désigner] précisant l'outil, l'usage et le lieu d'hébergement. Cet engagement figure au contrat ou dans un avenant, aux côtés des clauses de confidentialité existantes.

Pour un travailleur indépendant, seules les règles de sécurité et de confidentialité de la présente charte lui sont rendues applicables par son contrat : des consignes détaillées sur la façon d'exécuter sa mission pourraient faire présumer un lien de subordination (article L8221-6 du code du travail).

14. Journalisation et contrôle des usages

Les comptes professionnels des outils listés peuvent conserver l'historique des requêtes et des réponses. Les personnes chargées de l'administration informatique des outils n'y accèdent que pour la sécurité, le traitement d'un incident signalé ou la vérification du respect de la présente charte, sous le contrôle de [Référent IA à désigner]. Cet accès est proportionné au but recherché (article L1121-1 du code du travail) et ne porte pas sur les contenus identifiés comme personnels. Ces données sont conservées [durée à compléter]. Chaque salarié est informé de ce dispositif avant sa mise en service (article L1222-4 du code du travail ; articles 13 et 14 du RGPD).

15. Manquements

Le non-respect de la présente charte peut donner lieu à une mesure disciplinaire, dans le respect de la procédure prévue par le code du travail, une fois la charte entrée en vigueur selon la clause « Opposabilité ». Une erreur involontaire signalée n'est pas une faute. La dissimulation d'un incident et le contournement délibéré des règles ci-dessus constituent des manquements. Pour les prestataires, le manquement relève du contrat qui les lie à l'entreprise.

16. Règles propres à vos usages

- **Rédaction et synthèse internes.** Un document produit avec l'aide d'une IA et destiné à circuler en interne porte la mention de cette aide, afin que le lecteur sache ce qui a été relu et ce qui ne l'a pas été.
- **Échanges avec les clients.** Toute personne qui échange avec un système d'IA de l'entreprise en est informée au plus tard au début de l'échange. Si l'entreprise a développé ce système ou l'a fait développer sous son nom, cette information est une obligation de l'article 50, paragraphe 1, du règlement (UE) 2024/1689, applicable depuis le 2 août 2026 ; sinon, c'est une règle de l'entreprise. Une réponse rédigée par une IA et envoyée sous la signature d'un salarié est relue par ce salarié, qui en répond.

17. Classement des usages

Niveau	Exemples	Règle

Libre	Reformulation, traduction, brouillon, recherche d'idées, sur des contenus sans donnée confidentielle ni personnelle	Vérification par l'auteur
Sous validation	Contenu envoyé à l'extérieur, document engageant l'entreprise, traitement de données internes, action exécutée par un agent	Validation par une personne nommée avant envoi ou exécution
Interdit	Données listées à la clause 6 saisies hors environnement contractualisé validé par [Référent IA à désigner], outil absent de la liste, compte personnel, déduction des émotions d'un salarié ou d'un candidat, décision individuelle sans intervention humaine	Interdiction, signalement à [Référent IA à désigner]

18. Formation et maîtrise de l'IA

Chaque personne concernée suit une session de formation avant d'utiliser les outils listés plus haut. Elle couvre la présente charte, la rédaction de consignes, la reconnaissance d'un résultat faux, les données interdites en saisie et la conduite à tenir en cas d'incident. Les dates et la liste des participants sont conservées. Cette disposition répond à l'article 4 du règlement (UE) 2024/1689, applicable depuis le 2 février 2025. Dans sa rédaction issue du règlement (UE) 2026/1744, en vigueur depuis le 27 juillet 2026, il demande aux fournisseurs et aux déployeurs de prendre des mesures pour favoriser le développement de la maîtrise de l'IA par leur personnel et par les autres personnes qui utilisent les systèmes d'IA pour leur compte, en tenant compte de leurs connaissances, de leur expérience et du contexte d'utilisation. Il ne contraint pas à garantir un niveau spécifique de maîtrise par individu.

19. Signalement

Toute erreur, fuite de donnée, action inattendue d'un agent ou usage imprévu est signalé à [Référent IA à désigner] sans délai, et au plus tard le jour même. Le fait de signaler de bonne foi n'est jamais sanctionné, et une erreur involontaire signalée n'est pas une faute. Le signalement ne fait pas obstacle à l'examen des faits signalés. Le silence, lui, expose l'entreprise.

20. Suivi

La direction réexamine la présente charte au moins une fois par an, ainsi qu'à chaque nouvel outil déployé. La charte porte un numéro de version et une date.

Les effets de l'usage de l'IA sur le travail (charge, organisation, compétences, risques psychosociaux) sont pris en compte dans l'évaluation des risques professionnels et dans le document unique (articles L4121-3 et R4121-1 du code du travail).

21. Opposabilité

La présente charte comporte des obligations générales et permanentes dans les matières mentionnées aux articles L1321-1 (santé et sécurité, discipline et sanctions) et L1321-2 du code du travail. En application de l'article L1321-5, un tel document est, en toute hypothèse, soumis aux règles de procédure du règlement intérieur, même lorsque l'entreprise n'en a pas. Sa mise en œuvre suppose donc, dans cet ordre : sa communication par tout moyen aux personnes ayant accès aux lieux de travail ou aux locaux où se fait l'embauche (article R1321-1) ; sa communication en deux exemplaires à l'inspection du travail (article R1321-4) en même temps que la publicité ; une entrée en vigueur à une date postérieure d'un mois à l'accomplissement des formalités de publicité (article L1321-4). Chaque personne concernée reçoit la charte et en accuse réception. Cet accusé de réception atteste la remise : il ne modifie pas le contrat de travail.

Accusé de réception

Je soussigné(e) ....., fonction ....., reconnais avoir reçu la présente charte et en avoir pris connaissance.

Fait à ..... , le ..... / ..... / .....
Signature de la personne concernée :

Pour [Raison sociale] : [Référent IA à désigner], signature :

Annexe 1 · Trace de conformité

- Registre des outils : nom, éditeur, usage, lieu d'hébergement, cadre de transfert, contrat de sous-traitance, responsable, date de validation.
- Liste des personnes formées, date de la session, points couverts.
- Accusés de réception de la charte, preuve de sa publicité et de sa communication à l'inspection du travail, avis du CSE s'il existe.
- Journal des signalements et des suites données.
- Date du dernier réexamen de la charte et numéro de version.

Annexe 2 · À faire valider par votre conseil

- La procédure d'opposabilité retenue, au regard de votre effectif et de la présence d'un CSE, y compris le régime actuel du dépôt au greffe : depuis le 28 mai 2026, date d'entrée en vigueur de la loi n° 2026-403 de simplification de la vie économique, l'article L1321-4 ne le mentionne plus, mais l'article R1321-2 n'a pas été abrogé ; la fiche du ministère du Travail renvoie à un article R1321-12, introuvable dans le Code du travail, vraisemblablement l'article R1321-2.
- La validation effective de chaque outil listé : compte fourni par l'entreprise, contrat avec l'éditeur, réglages de conservation et d'entraînement.
- La qualification éventuelle de vos outils RH au titre de l'annexe III du règlement (UE) 2024/1689, et votre statut de déployeur ou de fournisseur (articles 3 et 25).

- Le cadre de transfert hors Union européenne de chaque outil retenu.
- Le régime des sanctions en cas de manquement, en l'absence de règlement intérieur.

Sources

- Règlement (UE) 2024/1689 sur l'intelligence artificielle : articles 3, 4, 5, 6, 25, 26, 27, 50, 99, 111, 113, annexes I et III. EUR-Lex. Version modifiée par le règlement (UE) 2026/1744, en vigueur depuis le 27 juillet 2026. EUR-Lex.
- Code du travail : articles L1121-1, L1221-8, L1222-4, L1311-2, L1321-1, L1321-2, L1321-4, L1321-5, R1321-1, R1321-2, R1321-4, L2311-2, L2312-1, L4121-3, R4121-1 et L8221-6 (Code du travail numérique, ministère du Travail). Fiche Le règlement intérieur, qui signale la suppression de la mention du dépôt au greffe par la loi n° 2026-403 de simplification de la vie économique, entrée en vigueur le 28 mai 2026.
- Règlement (UE) 2016/679 (RGPD) : articles 5, 6, 9, 13, 14, 22, 24, 28, 30, 32, 33, 34, 35, 37, 38 et chapitre V sur les transferts. EUR-Lex.
- CNIL et Conseil de l'IA et du numérique, note exploratoire sur l'IA agentique et les données personnelles, 20 juillet 2026. CNIL.
- CNIL, Les questions-réponses sur l'utilisation d'un système d'IA générative, 18 juillet 2024, qui recommande d'encadrer cet usage « par des politiques ou chartes internes, définissant clairement les usages autorisés et les usages interdits ». CNIL.
- ANSSI, Recommandations de sécurité pour un système d'IA générative, 29 avril 2024, recommandations R9, R31, R34 et R35 (Licence Ouverte 2.0). ANSSI.
- Cour de cassation, Charte éthique relative à l'utilisation des systèmes d'intelligence artificielle, arrêtée au 30 septembre 2026 (principes 1 à 3).

> **Note de transmission, à supprimer avant diffusion.** Document généré le [date de la version], sur l'état du droit à cette date. Ce contenu n'a pas été relu par un avocat : chaque règle renvoie à sa source. Les sanctions du règlement sur l'IA (chapitre XII) s'appliquent depuis le 2 août 2025, et les obligations de l'article 50 depuis le 2 août 2026 (le 2 décembre 2026 pour le marquage des contenus par les fournisseurs de systèmes mis sur le marché avant le 2 août 2026, article 111, paragraphe 4). Pour un manquement à l'article 50, l'amende peut atteindre 15 millions d'euros ou 3 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu ; pour une PME, c'est le montant le plus faible des deux (article 99, paragraphes 4 et 6), règle étendue aux petites entreprises à moyenne capitalisation (paragraphe 6 bis). Chaque État membre fixe le régime des sanctions (article 99, paragraphe 1). Ce document constitue une base de travail et non un avis juridique : faites-le relire par votre conseil avant diffusion, en particulier sur le volet droit social.
>
> Généré depuis romainbailleul.fr/generateur-charte-ia