

Charte d'utilisation de l'intelligence artificielle générative

[Modèle pour une entreprise de 20 salariés · à jour au 10 octobre 2026 : ligne à supprimer]

[Raison sociale], [forme juridique], [adresse du siège]

Version [1.0] du [date] · complète la charte d'utilisation des moyens informatiques et des outils numériques du [date]

[Le cas échéant : avis du comité social et économique du [date] ·] communication à l'inspection du travail et diffusion au personnel le [date] · [le cas échéant : dépôt au greffe du conseil de prud'hommes de [ville] le [date] ·] entrée en vigueur le [date, au moins un mois après ces formalités]

À lire avant d'utiliser ce modèle (page à supprimer)

Nous avons rédigé ce modèle chez KERIONIS, prestataire informatique à Crevin, en Ile-et-Vilaine, en complément de notre modèle de charte informatique. Il vise une entreprise fictive de 20 salariés dotée d'un CSE : bureaux, postes Windows, Microsoft 365, quelques salariés en télétravail, prestataire informatique extérieur. Il s'appuie notamment sur le règlement européen sur l'intelligence artificielle (règlement (UE) 2024/1689, modifié par le règlement (UE) 2026/1744), le RGPD, le Code du travail et les recommandations de la CNIL, de l'ANSSI et de Cybermalveillance.gouv.fr, dans leur état au 10 octobre 2026. Vous pouvez le reprendre et l'adapter librement.

Ce que demande le règlement européen. L'entreprise qui fait utiliser des outils d'IA à ses salariés pour le travail est « déployeur ». L'article 4 s'applique depuis le 2 février 2025 ; dans sa rédaction en vigueur depuis le 27 juillet 2026, il demande de prendre des mesures pour « favoriser » la maîtrise de l'IA par le personnel, sans niveau garanti par personne, et la Commission n'exige aucun certificat. Il ne figure pas parmi les manquements pour lesquels le règlement fixe un plafond d'amende (article 99, paragraphe 4) ; une sanction ne pourrait venir que du droit national, et au 10 octobre 2026 aucune loi française n'a désigné d'autorité de contrôle ni prévu de sanction. La CNIL recommande une charte qui liste les usages autorisés et interdits.

L'adapter. Remplacez le logo et tout ce qui figure entre crochets et surligné, puis tranchez les options : niveau « Confidentiel » à l'article 4, mention de l'IA à l'article 7, usage personnel à l'article 12. Remplissez le registre de l'annexe A avant l'adoption : un registre vide interdit tout outil (article 3). Interdire sans proposer d'outil pousse les usages hors de vue, et l'ANSSI relève que les usages non encadrés aggravent le risque de fuite. Les contrôles de l'article 12 doivent correspondre aux réglages réels des outils.

Avec la charte informatique. Ce modèle renvoie à notre modèle de charte informatique : il en précise l'article 12 et s'appuie sur ses règles de mots de passe, de confidentialité, de signalement des incidents, de contrôle et de sanction. Dans la charte informatique, renvoyez à l'annexe A ci-après la ligne « Intelligence artificielle » de l'annexe C, et à l'article 12 de la charte IA la dernière puce de l'article 20 et la ligne « Historique des outils d'IA » de l'annexe D. Alignez aussi son article 12 : la charte IA interdit dans tout outil, même autorisé, les informations du niveau « Interdit » (mots de passe, codes et clés, données de santé et autres données de l'article 9 du RGPD, coordonnées bancaires complètes, pièces d'identité). Si votre charte informatique ne suit pas notre modèle, vérifiez le numéro de chaque article et annexe cités ; sans charte informatique, remplacez chaque renvoi par la règle correspondante.

L'adopter dans les formes. Une charte qui pose des interdictions et annonce des sanctions contient des obligations générales et permanentes en matière de discipline. Selon la lettre de l'article L1321-5 du Code du travail, elle suit alors les règles du règlement intérieur, même dans une entreprise de moins de 50 salariés qui n'en a pas ; aucune décision publiée n'a tranché ce cas. Par prudence, suivez la procédure de l'article L1321-4, comme pour la charte informatique :

- avis préalable du comité social et économique, s'il existe (à partir de 11 salariés) ;
- diffusion au personnel par tout moyen (affichage, intranet, remise individuelle) ;
- communication à l'inspection du travail, en deux exemplaires, avec l'avis du CSE, en même temps que la diffusion ;
- texte rédigé en français (article L1321-6) ;
- entrée en vigueur au moins un mois après ces formalités ; toute modification suit le même chemin.

Si les deux chartes sont adoptées ensemble, menez ces formalités en même temps. Le dépôt au greffe du conseil de prud'hommes n'est plus prévu par la loi depuis le 28 mai 2026, mais l'article R1321-2 figure toujours comme en vigueur sur Légifrance. Par prudence, vous pouvez effectuer ce dépôt. Le délai d'un mois court alors à partir de la dernière formalité, dépôt compris (article R1321-3).

La voie la plus sûre, à faire valider par votre conseil, est d'adopter un règlement intérieur, facultatif sous 50 salariés, et d'y annexer les deux chartes : des règles posées hors d'un règlement intérieur ou d'une note de service régulièrement adoptée ont été jugées inopposables. La signature de chaque salarié ne dispense pas de ces formalités ; l'attestation de l'annexe E prouve seulement la remise de la charte et l'information de chacun.

Ce que la charte ne remplace pas.

- le contrat de sous-traitance (article 28 du RGPD) avec l'éditeur de chaque outil qui traite des données personnelles ;
- le registre des traitements et, si nécessaire, l'analyse d'impact ;
- les règles d'une profession tenue au secret (avocats, experts-comptables, professionnels de santé) : le modèle de charte du Barreau de Paris, fondé sur la signature, vise des avocats et ne se transpose pas tel quel à des salariés ;
- l'examen des outils de recrutement ou d'évaluation des salariés, classés à haut risque et soumis à des obligations propres à partir du 2 décembre 2027.

N'y ajoutez ni engagement de « garantir » la maîtrise de l'IA, ni clause générale de surveillance des échanges avec l'IA, ni amende ni retenue sur salaire.

Ce modèle n'est pas un avis juridique. Faites relire votre version par votre conseil avant de l'adopter. Revoyez-la à chaque changement d'outil et à chaque évolution attendue : loi française désignant les autorités de contrôle (projet de loi n° 2518, au stade de l'examen en commission en première lecture au 10 octobre 2026), recommandations de la CNIL sur l'IA au travail (annoncées, non datées), nouvelles interdictions du 2 décembre 2026, règles sur l'IA à haut risque du 2 décembre 2027.

Modèle proposé gratuitement par KERIONIS, Crevin (Ille-et-Vilaine) · 06 77 40 79 55 · contact@kerionis.fr · <https://www.kerionis.fr/charte-ia-entreprise>

Sommaire

Préambule

1. Objet et champ d'application · 2. Définitions · 3. Outils et comptes autorisés · 4. Classification des données et données interdites
5. Usages permis et vérification humaine · 6. Décisions concernant des personnes et usages interdits · 7. Mention de l'usage de l'IA et contenus publiés
8. Propriété intellectuelle et confidentialité · 9. Sécurité des comptes, extensions et agents · 10. Incidents et signalement
11. Formation et maîtrise de l'IA · 12. Contrôles, traçabilité et information des utilisateurs · 13. Manquements et sanctions
14. Signalements protégés et représentants du personnel · 15. Entrée en vigueur, diffusion et révision
Annexes : A. Registre des outils d'IA autorisés · B. Puis-je confier cette donnée à l'IA ? · C. Liste de contrôle avant de publier ou d'envoyer · D. Demande d'un nouvel outil d'IA · E. Attestation de remise

Préambule

[Raison sociale] permet à son personnel d'utiliser des outils d'intelligence artificielle générative pour rédiger, reformuler, résumer, traduire ou chercher des idées. Ces outils font gagner du temps. Ils peuvent aussi se tromper avec assurance, et ce qu'on leur confie est traité, parfois conservé, par leur éditeur.

La présente charte fixe les règles qui permettent de s'en servir sans exposer les clients, les salariés ni l'entreprise, et informe chacun des contrôles en place et de ses droits. Elle complète la charte d'utilisation des moyens informatiques et des outils numériques du [date] (ci-après « la charte informatique »), dont elle précise l'article 12 ; les deux documents s'appliquent ensemble et, pour l'usage de l'IA, la présente charte prévaut en cas de divergence.

Elle comporte des obligations générales et permanentes en matière de discipline : à ce titre, elle a été [le cas échéant : soumise à l'avis du comité social et économique le [date],] [le cas échéant : déposée au greffe du conseil de prud'hommes de [ville] le [date],] communiquée à l'inspection du travail et portée à la connaissance du personnel le [date] par [affichage et publication sur l'intranet]. Elle entre en vigueur le [date]. [Si l'entreprise dispose d'un règlement intérieur : elle y est annexée et en fait partie.] Les règles écrites au présent s'imposent à tous. La charte est disponible sur [emplacement : intranet, dossier partagé].

Article 1. Objet et champ d'application

La charte encadre l'usage des outils d'intelligence artificielle générative pour le travail. Elle vise à protéger les données de l'entreprise, de ses clients et de ses salariés, à faire vérifier tout contenu produit avec l'IA par une personne qui en répond, et à organiser la formation du personnel.

Personnes concernées. Toute personne qui utilise un outil d'IA pour le compte de l'entreprise : salariés quel que soit leur contrat, apprentis, stagiaires, intérimaires. Les prestataires extérieurs qui utilisent l'IA sur des données de l'entreprise y sont tenus par une clause de leur contrat [à vérifier dans les contrats en place].

Outils concernés. Tout outil d'IA générative, quel que soit son mode d'accès : service en ligne, application, extension de navigateur, agent, ou fonction d'IA intégrée à un logiciel déjà utilisé (messagerie, bureautique, visioconférence, logiciel métier), qui suit les mêmes règles qu'un outil distinct.

Lieux et moments. La charte s'applique dans les locaux, en télétravail et en déplacement, quel que soit l'appareil, dès que l'outil sert au travail ou reçoit des données de l'entreprise. Elle ne régit pas l'usage privé de l'IA, sans lien avec l'entreprise ni avec ses données.

Article 2. Définitions

- **Utilisateur** : toute personne visée à l'article 1.

- **Outil d'IA** : service, logiciel, extension ou fonction d'IA générative, c'est-à-dire qui produit du texte, des images, du son, de la vidéo ou du code à partir d'une demande de l'utilisateur.
- **Outil autorisé** : outil inscrit au registre de l'annexe A, dans l'offre que ce registre indique, utilisé avec le compte professionnel, pour les usages et dans la limite du niveau de données qu'il fixe.
- **Compte professionnel** : compte ouvert par l'entreprise ou à sa demande, avec l'adresse professionnelle nominative de l'utilisateur.
- **Requête** : tout ce qui est transmis à un outil d'IA (texte saisi ou collé, fichier, image, capture d'écran, dictée, contenu lu par un connecteur).
- **Agent d'IA** : outil d'IA capable d'agir seul pour l'utilisateur, par exemple exécuter des commandes, piloter le navigateur, envoyer des messages ou manipuler des fichiers.
- **Hypertrucage** : image, son ou vidéo générés ou manipulés par l'IA, qui ressemblent à des personnes, des objets, des lieux, des entités ou des événements existants et pourraient être perçus à tort comme authentiques ou véridiques (article 3, point 60, du règlement européen sur l'IA).
- **Prestataire informatique** : [nom du prestataire], au sens de l'article 3 de la charte informatique.
- **Référent IA** : [nom et fonction, par exemple le référent informatique], désigné par la direction pour tenir le registre de l'annexe A, répondre aux questions et recevoir les demandes et les signalements, en lien avec le prestataire informatique.

Article 3. Outils et comptes autorisés

Seuls les outils inscrits au registre de l'annexe A sont utilisés pour le travail, avec le compte professionnel, pour les usages et dans la limite du niveau de données que le registre fixe pour chacun. Tout autre outil, comme toute autre offre d'un outil inscrit (version gratuite ou grand public), est interdit pour le travail, même pour un usage qui paraît anodin.

L'utilisateur ne se sert jamais, pour le travail, d'un compte d'IA personnel ou ouvert avec une adresse personnelle. Il n'ouvre aucun compte d'IA avec son adresse professionnelle sans l'accord du référent IA, ne partage son compte avec personne et ne modifie pas les réglages fixés par l'entreprise (historique, réutilisation des données par l'éditeur, connecteurs, partage des conversations).

Ajout d'un outil. L'utilisateur qui a besoin d'un nouvel outil le demande au référent IA avec le formulaire de l'annexe D, sans essayer l'outil avec des données de l'entreprise. Avant toute inscription, l'entreprise examine avec son prestataire informatique les points de cette annexe, dont le contrat de sous-traitance prévu par l'article 28 du RGPD ; le registre fixe ensuite le niveau de données maximal et les réglages imposés.

Réexamen. Chaque outil est réexaminé au moins une fois par an, et sans attendre en cas de changement des conditions d'utilisation, de l'hébergement, des sous-traitants ou de l'actionnariat de l'éditeur, ou si une faille est connue (article 15).

Usages antérieurs. Les usages faits de bonne foi pour le travail avant l'entrée en vigueur de la présente charte ne sont pas reprochés, sauf s'ils contrevenaient déjà à la charte informatique alors en vigueur. Dans le mois qui suit l'entrée en vigueur, chaque utilisateur signale au référent IA les outils et comptes personnels dont il s'est servi. Il en supprime ensuite, avec son aide si besoin, les conversations et fichiers contenant des données de l'entreprise, une fois que le référent a vérifié avec la direction si des données personnelles transmises relèvent de l'article 10. Une transmission de données personnelles ainsi révélée est traitée comme un incident (article 10), sans être reprochée.

Article 4. Classification des données et données interdites

Avant toute requête, l'utilisateur détermine le niveau de l'information qu'il transmet, d'après son contenu, même en l'absence de marquage. En cas de doute, il retient le niveau supérieur et consulte le référent IA ; la grille de l'annexe B l'aide à décider. Les informations des niveaux « Confidentiel » et « Interdit » sont dites « données sensibles ».

Niveau	Ce qu'il recouvre	Règle
--------	-------------------	-------

Public	Information déjà publique ou destinée à être publiée sans restriction : site internet de l'entreprise, plaquette, offre d'emploi publiée, texte de loi.	Tout outil autorisé.
Interne	Information non publique qui ne permet d'identifier personne et ne contient rien de confidentiel : procédure générale, modèle de courrier vierge, question technique formulée sans nom.	Outils dont le niveau maximal au registre est « Interne » ou « Confidentiel ».
Confidentiel	Données personnelles (clients, prospects, salariés, candidats, fournisseurs) ; dossiers des clients ; contrats, devis, tarifs et conditions commerciales ; données financières, sociales et de paie ; projets non publics ; documents reçus sous engagement de confidentialité ou marqués « Confidentiel » ; [à adapter].	Seulement dans un outil que le registre autorise expressément pour ce niveau, et réduit au strict nécessaire. [Option : aucun outil n'est ouvert à ce niveau.]
Interdit	Mots de passe, codes, clés et jetons d'accès, codes de double authentification ; données de santé et autres données de l'article 9 du RGPD (origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques, données biométriques servant à identifier une personne, vie sexuelle ou orientation sexuelle) ; coordonnées bancaires complètes et pièces d'identité ; [données relatives aux condamnations pénales et aux infractions (article 10 du RGPD) ; numéro de sécurité sociale] ; [le cas échéant : informations couvertes par un secret professionnel].	Jamais, dans aucun outil d'IA, même autorisé.

Réduire au strict nécessaire. Même dans un outil autorisé, l'utilisateur ne transmet que ce que la tâche exige et remplace les noms par des mentions neutres (« le client », « la salariée A »). Une donnée pseudonymisée reste une donnée personnelle : quelques indices croisés (un montant, un nom de projet, une fonction rare) peuvent suffire à retrouver la personne ou le client.

Ces règles visent toute forme de requête, y compris un fichier entier dont seule une partie est utile ou une capture d'écran qui laisse voir une messagerie. Une saisie de données sensibles faite par erreur se signale aussitôt (article 10).

Article 5. Usages permis et vérification humaine

Usages possibles. Les outils autorisés peuvent notamment servir à reformuler ou corriger un texte, proposer un plan ou une première ébauche, résumer ou traduire un document dont le niveau le permet, expliquer une notion, une formule de tableur ou un message d'erreur. [Liste à adapter aux métiers de l'entreprise.]

Vérification. Un outil d'IA peut se tromper, inventer des faits ou des sources et reproduire des biais, avec assurance. Aucune production n'est donc utilisée telle quelle : avant de l'envoyer, de la publier ou de s'en servir pour décider, l'utilisateur la relit en entier et vérifie :

- les faits, chiffres, dates et noms, dans une source fiable ;
- l'existence des sources citées et ce qu'elles disent réellement ; un texte de loi ou une décision de justice se contrôle sur Légifrance ou sur le site officiel de la juridiction ;
- l'absence de passage repris d'une œuvre protégée (article 8) ;
- la cohérence du résultat avec ce qu'il sait du dossier, sans se fier à la qualité de la rédaction.

Responsabilité. L'utilisateur répond de ce qu'il produit avec l'IA comme de tout autre travail, et la décision finale appartient toujours à une personne. Une réponse de l'IA ne remplace ni l'avis d'un juriste ou d'un médecin, ni la validation d'un comptable.

Code informatique. Un code, un script ou une macro produits par l'IA ne sont exécutés qu'après avoir été relus et testés hors des données réelles. Un composant logiciel proposé par l'IA est vérifié à sa source officielle avant toute

installation, réservée au prestataire : une IA peut citer un composant inexistant, qu'un attaquant peut ensuite publier sous ce nom.

Continuité. Aucune tâche ne doit devenir impossible si l'outil d'IA est indisponible ou retiré.

Article 6. Décisions concernant des personnes et usages interdits

Aucune décision qui concerne une personne (salarié, candidat, client, fournisseur) n'est prise par un outil d'IA ni sur la seule base de sa réponse. Aucun outil d'IA ne sert à recruter, trier des candidatures, évaluer, promouvoir, sanctionner ou licencier un salarié, ni à lui attribuer des tâches, sans décision préalable de la direction, examen de l'outil (article 3), information préalable et expresse des candidats et des salariés concernés (articles L1221-8, L1222-3 et L1222-4 du Code du travail) et information de leurs représentants. Les obligations du règlement européen sur ces systèmes, pour la plupart classés à haut risque (annexe III, point 4), s'appliqueront le 2 décembre 2027.

Il est interdit d'utiliser un outil d'IA pour :

- déduire les émotions d'une personne sur le lieu de travail, par quelque moyen que ce soit ; fondée sur des données biométriques (visage, voix, gestes, frappe au clavier), cette pratique est interdite par le règlement européen depuis le 2 février 2025, sauf raisons médicales ou de sécurité ;
- représenter une personne réelle (image, vidéo, voix) sans son accord, ou produire un contenu sexiste, sexuel, dégradant ou discriminatoire visant quiconque ;
- se faire passer pour une autre personne, ou imiter sa voix ou sa manière d'écrire pour tromper un tiers ;
- contourner une règle de sécurité, une licence ou une protection technique, ou surveiller l'activité d'un collègue ;
- enregistrer, transcrire ou résumer automatiquement un appel ou une réunion sans en avoir informé au préalable tous les participants (article 20 de la charte informatique).

La diffusion, sans son consentement, d'un contenu généré représentant une personne, dont le caractère artificiel n'est ni évident ni signalé, est punie d'un an d'emprisonnement et de 15 000 euros d'amende, et de deux ans et 45 000 euros en ligne (article 226-8 du Code pénal). Le harcèlement moral et le harcèlement sexuel, interdits par le Code du travail (articles L1152-1 et L1153-1), le restent lorsqu'ils passent par un outil d'IA ; le Code pénal punit plus sévèrement le harcèlement sexuel commis au moyen d'un support numérique. Contacts utiles : annexe A de la charte informatique.

Article 7. Mention de l'usage de l'IA et contenus publiés

Ce que la loi impose. Depuis le 2 août 2026, l'article 50 du règlement européen sur l'IA oblige l'entreprise qui produit un hypertrucage avec un outil d'IA à indiquer, en le diffusant, qu'il a été généré ou modifié par une IA ; pour une œuvre manifestement artistique, satirique ou fictive, une mention adaptée suffit. Un texte généré ou modifié par une IA et publié pour informer le public sur des questions d'intérêt public porte la même indication, sauf s'il a fait l'objet d'une relecture humaine ou d'un contrôle éditorial et qu'une personne en assume la responsabilité éditoriale. L'information est claire et donnée au plus tard au premier contact avec le contenu.

Ce que l'entreprise décide en plus. [Option à trancher par la direction : garder, modifier ou supprimer les trois phrases qui suivent.] Une simple correction ou reformulation ne demande aucune mention. Un document remis à l'extérieur dont l'IA a produit l'essentiel porte la mention « Document rédigé avec l'assistance d'un outil d'IA générative et vérifié par [nom] ». L'utilisateur signale l'usage de l'IA à son responsable pour un travail dont elle a produit une part importante, et à tout client qui le demande ou dont le contrat l'exige.

Publications de l'entreprise. Aucun contenu produit avec l'IA n'est publié au nom de l'entreprise (site internet, réseaux sociaux, lettre d'information, publicité) sans la validation de [personne désignée par la direction] et la liste de contrôle de l'annexe C. Une image générée n'est jamais présentée comme une photographie réelle.

Article 8. Propriété intellectuelle et confidentialité

Contenus produits avec l'IA. Leur protection par le droit d'auteur reste incertaine. Selon un rapport de mission présenté en juillet 2026 au Conseil supérieur de la propriété littéraire et artistique (rapport qui n'engage que ses

auteurs), une production sans intervention humaine déterminante relève du domaine public ; seule une création où une personne a joué un rôle créatif actif peut être protégée, si elle est originale. Pour un logo, un nom de produit ou un slogan, l'utilisateur en parle d'abord à [la direction] et garde la trace de son travail (versions, requêtes, choix).

Droits des tiers. Une production de l'IA peut reproduire sans le signaler un texte, une image ou un logo protégés : avant toute exploitation à l'extérieur, l'utilisateur vérifie que l'entreprise en a les droits. Il ne soumet pas à un outil un document d'un tiers (étude achetée, ouvrage, contenu sous licence) si la licence ne le permet pas.

Créations des salariés. La charte n'opère aucune cession de droits. Le contrat de travail n'emporte pas, à lui seul, cession des droits d'auteur (article L111-1 du Code de la propriété intellectuelle), sauf régimes particuliers : les droits patrimoniaux sur les logiciels créés par un salarié dans ses fonctions sont dévolus à l'employeur, sauf stipulation contraire (article L113-9), et l'œuvre collective appartient, sauf preuve contraire, à la personne sous le nom de laquelle elle est divulguée (article L113-5).

Confidentialité. Transmettre une information à un outil d'IA revient à la confier à son éditeur : l'article 11 de la charte informatique et les engagements de confidentialité pris envers les clients s'appliquent aux requêtes. [Si l'entreprise ou certains salariés sont tenus à un secret professionnel :] aucune information couverte par ce secret n'est transmise à un outil d'IA ; sa révélation par la personne qui en est dépositaire est punie d'un an d'emprisonnement et de 15 000 euros d'amende (article 226-13 du Code pénal).

Article 9. Sécurité des comptes, extensions et agents

Comptes. Le compte professionnel d'un outil d'IA se protège comme la messagerie : mot de passe unique conforme à l'article 5 de la charte informatique, double authentification, [connexion par le compte professionnel de l'entreprise (authentification unique) lorsque l'outil le permet]. Un compte piraté livre tout l'historique des conversations : l'utilisateur ne s'y connecte que depuis un appareil de confiance, par les liens du registre ou l'application installée par le prestataire, jamais par un lien reçu ou sponsorisé.

Extensions, connecteurs et agents. Sans l'accord écrit de la direction et du prestataire informatique, il est interdit d'installer une extension ou une application d'IA, d'activer un agent ou de connecter un outil d'IA à la messagerie, à l'agenda, aux fichiers, au logiciel métier ou au navigateur. Une connexion autorisée ne reçoit que les droits nécessaires, vérifiés par le prestataire à l'activation puis [chaque mois]. Aucun agent n'envoie, ne paie, ne publie, ne modifie ni ne supprime quoi que ce soit sans validation de chaque action par l'utilisateur.

Injection de consignes. Un courriel, une page web ou un document venus de l'extérieur peuvent cacher des instructions destinées à l'IA qui les lit, par exemple ignorer les consignes de l'utilisateur ou envoyer un fichier. L'utilisateur ne demande donc jamais à un assistant d'agir (envoyer, payer, modifier, supprimer) à partir d'un tel contenu ; il peut le lui faire résumer, et lit ce résumé avec prudence. Si l'outil propose de cliquer sur un lien, de saisir un mot de passe ou de faire ce qui n'a pas été demandé, l'utilisateur s'arrête et le signale (article 10).

Article 10. Incidents et signalement

L'utilisateur signale sans délai au référent IA et au prestataire informatique, par téléphone ou de vive voix (article 19 et annexe A de la charte informatique) :

- une donnée saisie dans un outil autorisé au-delà du niveau maximal que lui fixe le registre, ou toute donnée de l'entreprise saisie dans un outil non autorisé ;
- un mot de passe, un code ou une clé d'accès transmis à un outil d'IA ;
- une connexion suspecte ou une conversation inconnue dans l'historique ;
- une action non demandée d'un outil ou d'un agent, une réponse qui invite à cliquer, à payer ou à transmettre des informations ;
- un contenu produit avec l'IA, déjà diffusé, qui se révèle faux ou contraire à la charte.

Il ne supprime pas la conversation avant d'en avoir parlé au référent : elle montre ce qui a été transmis. Un mot de passe ou un code saisi est changé aussitôt, depuis un appareil de confiance.

La transmission non autorisée de données personnelles à un service tiers peut constituer une violation de données au sens du RGPD : l'entreprise la consigne alors dans son registre interne des violations et, sauf si elle n'est pas

susceptible d'engendrer un risque pour les personnes, la notifie à la CNIL dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance ; si le risque est élevé, elle en informe aussi les personnes concernées. Le signalement est donc urgent ; il n'est jamais reproché (article 13).

Article 11. Formation et maîtrise de l'IA

Conformément à l'article 4 du règlement européen sur l'IA, l'entreprise prend des mesures pour favoriser la maîtrise de l'IA par son personnel et par les personnes qui utilisent l'IA pour son compte, en tenant compte de leurs connaissances, de leur expérience et du contexte d'usage :

- une sensibilisation avant l'ouverture de tout accès à un outil autorisé, puis [chaque année] : fonctionnement et limites de l'IA générative, outils du registre et réglages imposés, classification des données (article 4 de la présente charte), risques propres (fuite de données, compte piraté, injection de consignes), conduite à tenir en cas d'incident ;
- [une formation complémentaire pour les usages propres à certains postes, à adapter] ;
- la remise de la présente charte à chaque nouvel arrivant ;
- [un temps d'échange régulier sur les usages et les erreurs rencontrées, à adapter].

L'entreprise consigne ces actions dans un registre des sensibilisations (date, contenu, participants). Les intérimaires, stagiaires et prestataires reçoivent les informations utiles à leur mission. Chacun peut demander une formation complémentaire au référent IA.

Article 12. Contrôles, traçabilité et information des utilisateurs

Dispositifs en place. Tout dispositif de contrôle est annoncé avant sa mise en œuvre et proportionné à sa finalité (articles L1121-1 et L1222-4 du Code du travail). Pour la sécurité des données et, en cas d'anomalie ou d'incident, la vérification du respect de la charte, l'entreprise met en œuvre les dispositifs suivants, et aucun autre [liste à ajuster aux réglages réels] :

- historique des requêtes et des réponses du compte professionnel, conservé par chaque outil autorisé pendant [durée] ;
- journalisation des connexions aux outils et des actions des connecteurs et agents autorisés ;
- rapports d'usage de la console d'administration [noms masqués lorsque l'outil le permet] (utilisateurs actifs, volume), qui servent aussi à gérer les licences, sans lecture des conversations ;
- [le cas échéant : blocage des sites d'IA absents du registre par le filtrage de la navigation décrit à l'article 20 de la charte informatique].

Accès aux conversations. Les conversations d'un compte professionnel sont présumées professionnelles, sauf celles que l'utilisateur a identifiées comme personnelles [par exemple « Personnel » dans leur titre, si l'outil le permet] : celles-ci ne sont ouvertes que dans les conditions de l'article 20 de la charte informatique, y compris avec l'option A. [Option A : tout usage personnel des outils d'IA de l'entreprise est interdit.] [Option B : un usage personnel ponctuel est toléré ; l'utilisateur identifie ces conversations comme personnelles quand l'outil le permet et n'y confie aucune information sensible.] Seul [le prestataire, sur demande écrite de la direction] consulte l'historique d'un utilisateur [moyen d'accès : console d'administration ou outil de conformité de l'éditeur ; certaines offres n'en donnent aucun], et seulement en cas d'incident, de transmission suspectée de données sensibles ou d'anomalie précise, après examen des données globales ; il ne transmet à la direction que les éléments utiles à la vérification. L'utilisateur en est informé dès que la vérification n'en est plus compromise, et avant toute décision le concernant.

Ce que l'entreprise ne fait pas. Elle ne se sert ni des historiques, ni des journaux, ni des rapports d'usage pour mesurer la productivité ou évaluer les salariés, et n'analyse pas leurs requêtes pour en déduire leurs émotions. Les engagements de l'article 20 de la charte informatique s'appliquent aussi aux outils d'IA.

Information et droits. Responsable du traitement : [raison sociale, adresse] · contact : [nom, courriel].

Dispositif	Finalité	Base légale	Conservation	Destinataires
------------	----------	-------------	--------------	---------------

Historique des requêtes et des réponses	Service rendu à l'utilisateur ; sécurité, enquête après incident, vérification du respect de la charte en cas d'anomalie	Intérêt légitime : fournir l'outil, protéger les données, faire respecter la charte	[durée]	Utilisateur ; prestataire en cas d'incident ou d'anomalie ; direction pour les seuls éléments utiles à la vérification ; éditeur, sous-traitant [nom, pays d'hébergement]
Journaux de connexion et d'actions	Sécurité, enquête après incident, vérification du respect de la charte en cas d'anomalie	Obligation légale de sécurité (article 32 du RGPD) pour la sécurité ; intérêt légitime (faire respecter la charte) pour la vérification en cas d'anomalie	[entre 6 et 12 mois]	Prestataire, référent IA
Rapports d'usage globaux ; registre des sensibilisations	Gestion des licences ; trace des mesures de l'article 4 du règlement européen	Intérêt légitime : gérer les outils, documenter ces mesures	[durée]	Référent IA, direction

[Transferts hors de l'Union européenne et garanties, ou absence de transfert.] Chaque utilisateur exerce sur ces données, historique de ses conversations compris, les droits prévus par le RGPD, dans les conditions de l'annexe D de la charte informatique, sous réserve des droits des personnes dont les données figurent dans ces conversations (article 15, paragraphe 4, du RGPD). Il peut saisir la CNIL d'une réclamation (cnil.fr). Ces traitements figurent au registre des traitements. Les membres du CSE disposent d'un droit d'alerte en cas d'atteinte injustifiée aux droits des personnes ou aux libertés individuelles. Tout nouveau dispositif est ajouté au présent article avant sa mise en service.

Article 13. Manquements et sanctions

Un manquement d'un salarié à la présente charte peut entraîner l'une des sanctions prévues par [le règlement intérieur ou l'article 24 de la charte informatique], proportionnée à la gravité des faits et prononcée après la procédure des articles L1332-1 à L1332-5 du Code du travail, qui garantit les droits de la défense. [Sans règlement intérieur ni charte informatique adoptée, reprendre ici l'échelle (avertissement, mise à pied disciplinaire de [3] jours au plus, mutation, rétrogradation, licenciement) et les droits de la défense : griefs notifiés par écrit, entretien préalable lorsqu'il est requis, assistance par une personne de son choix appartenant au personnel.] Aucune amende ni autre sanction pécuniaire ne peut être prononcée (article L1331-2 du Code du travail).

Une erreur involontaire signalée sans délai n'est pas sanctionnée. Seul peut l'être un manquement délibéré ou répété, par exemple l'usage d'un compte personnel ou d'un outil non autorisé avec des données de l'entreprise après la sensibilisation, la transmission volontaire de données classées « Interdit » ou la dissimulation d'un incident.

Pour une personne qui n'est pas salariée de l'entreprise, un manquement est signalé à son employeur, à son établissement ou à sa société, et peut entraîner la fin de son accès et de sa mission dans les conditions de son contrat ou de sa convention. Un accès peut être suspendu à titre conservatoire si la sécurité des données l'exige. Ces mesures s'entendent sans préjudice des poursuites civiles ou pénales encourues.

Article 14. Signalements protégés et représentants du personnel

Aucune disposition de la présente charte, notamment les règles sur la transmission de données et les obligations de confidentialité, ne fait obstacle à un signalement ou à une divulgation dans les conditions prévues par les articles 6 à 8 de la loi n° 2016-1691 du 9 décembre 2016 (dite loi « Sapin II »), qui protège les lanceurs d'alerte. La charte ne fait pas non plus obstacle à l'information des représentants du personnel ni au témoignage de faits de

harcèlement ou de discrimination. Les canaux de signalement et l'interdiction des représailles figurent à l'article 25 de la charte informatique.

Article 15. Entrée en vigueur, diffusion et révision

La charte entre en vigueur le [date], au moins un mois après l'accomplissement des formalités rappelées dans le préambule. L'attestation de l'annexe E prouve sa remise.

Elle est revue au moins une fois par an et à chaque changement important d'outil, d'organisation ou de réglementation. Toute modification de ses règles suit la procédure d'adoption.

Le référent IA tient à jour le registre de l'annexe A. L'inscription d'un outil à ce registre n'exige pas la procédure d'adoption ; le retrait d'un outil et toute restriction nouvelle la suivent. En cas de risque pour la sécurité ou les données (faible connue, changement des conditions de l'éditeur), [la direction] peut toutefois désactiver sans délai l'accès à un outil, à titre conservatoire ; elle en informe les utilisateurs et le CSE, puis rétablit l'accès ou engage le retrait selon la procédure d'adoption.

Annexe A. Registre des outils d'IA autorisés

Tenu par le référent IA, version du [date]. Tout outil absent de ce registre est interdit pour le travail. Niveaux de données : article 4. Réexamen au moins annuel (article 3).

Outil et offre souscrite	Accès	Usages prévus	Niveau maximal	Réglages imposés	Contrat, hébergement, validation
[Assistant conversationnel : nom de l'outil et de l'offre professionnelle souscrite]	[lien ou application ; compte professionnel ; double authentification]	[rédaction, reformulation, résumé, traduction]	[Interne]	[historique : [durée] ; réutilisation des données désactivée]	[contrat de sous-traitance du [date] ; hébergement [pays] ; validé le [date]]
[Fonction d'IA intégrée à un logiciel déjà utilisé : bureautique, messagerie, logiciel métier]				[accès aux fichiers limité à [périmètre]]	
[Outil de traduction]					
[Transcription et résumé de réunions, après information de tous les participants]					

Fonctions d'IA désactivées ou non autorisées. [Liste, par exemple un agent ou un connecteur vers la messagerie.]

Outils suspendus ou retirés. [Nom de l'outil, date, motif.]

Annexe B. Puis-je confier cette donnée à l'IA ?

À garder près du poste. En cas de doute, ne saisissez rien et appelez le référent IA : [numéro].

Cinq questions avant chaque requête

Question	Conséquence
1. L'outil figure-t-il au registre de l'annexe A, et suis-je connecté avec mon compte professionnel ?	Si non : je ne saisis rien.
2. Ma requête contient-elle un mot de passe, un code, une donnée de santé ou une autre donnée de l'article 9 du RGPD, des coordonnées bancaires complètes, une pièce d'identité ?	Si oui : niveau « Interdit », je ne la saisis dans aucun outil.
3. Permet-elle d'identifier une personne ou un client, même indirectement (nom, fonction rare, montant) ? Contient-elle un contrat, un tarif, une donnée financière ou sociale, un projet non public ?	Si oui : niveau « Confidentiel », seulement dans un outil autorisé pour ce niveau ; à défaut d'un tel outil, je retire ces éléments ou je renonce.
4. Cette information est-elle publiée, ou destinée à l'être, sans restriction ?	Si oui : niveau « Public ». Si non : niveau « Interne » au moins.
5. Le niveau de ma requête dépasse-t-il le niveau maximal de l'outil dans le registre ?	Si oui : je ne saisis rien. Si non : je peux saisir, puis je vérifie le résultat (article 5).

Exemples

Situation	Niveau	Réponse
Reformuler un texte du site internet de l'entreprise	Public	Oui, dans tout outil autorisé.
Corriger un courriel de relance qui contient le nom du client et le montant dû	Confidentiel	Seulement dans un outil autorisé pour ce niveau ; sinon, remplacez nom et montant par « [client] » et « [montant] », puis complétez vous-même.
Préparer l'entretien annuel d'un salarié à partir de ses résultats	Confidentiel	Non, sauf outil retenu pour cet usage dans les conditions de l'article 6 (décision de la direction, examen de l'outil, information préalable) : données d'un salarié et usage lié à son évaluation.
Faire analyser un arrêt de travail ou un certificat médical	Interdit	Jamais.
Faire résumer un courriel reçu, puis demander à l'assistant d'envoyer la réponse ou d'agir	Selon le contenu	Le résumé et un projet de réponse relu sont possibles selon le niveau ; aucun envoi ni aucune action n'est confié à l'assistant à partir de ce contenu (article 9).

Annexe C. Liste de contrôle avant de publier ou d'envoyer

Obligatoire pour toute publication au nom de l'entreprise : la liste remplie est remise à la personne qui valide (article 7). Aide-mémoire pour tout autre contenu produit en tout ou partie avec l'IA qui sort de l'entreprise ou sert à décider.

Point vérifié	Oui	Sans objet
J'ai relu le contenu en entier et je peux en expliquer chaque passage.	☐	☐
Les faits, chiffres, dates et noms ont été vérifiés dans une source fiable.	☐	☐
Chaque source citée existe et dit ce que le contenu lui attribue ; les références juridiques ont été vérifiées sur Légifrance ou sur le site officiel de la juridiction.	☐	☐
Le contenu ne contient aucune donnée sensible qui n'a pas à y figurer, et les requêtes qui l'ont produit respectaient l'article 4.	☐	☐
Le contenu ne reprend ni texte, ni image, ni logo protégés, ou l'entreprise dispose des droits nécessaires.	☐	☐
Aucune personne réelle n'est représentée sans son accord, et aucune image générée n'est présentée comme une photographie réelle.	☐	☐
Un hypertrucage porte, dès le premier contact, la mention de son caractère artificiel ; un texte d'information du public sur une question d'intérêt public est relu sous la responsabilité éditoriale d'une personne, ou porte cette mention.	☐	☐
La mention décidée par l'entreprise (article 7) figure sur le document, s'il y a lieu.	☐	☐
Le contenu n'engage pas l'entreprise au-delà de ce qu'elle a validé : prix, délais, garanties, conditions contractuelles.	☐	☐

Relu et validé par [nom, fonction], le [date] · contenu concerné : [titre, destinataire ou adresse de publication]

Annexe D. Demande d'un nouvel outil d'IA

À remplir par le demandeur

Demandeur, service, date	
Nom de l'outil, éditeur, adresse du site	
Offre envisagée, nombre de comptes, coût	
Besoin : ce que l'outil permettrait de faire, et pourquoi les outils du registre ne suffisent pas	
Données qui seraient transmises, et niveau le plus élevé selon l'article 4	
Connexions demandées (messagerie, agenda, fichiers, navigateur, logiciel métier) et actions que l'outil ferait seul	
Personnes qui l'utiliseraient	

Examen par le référent IA et le prestataire informatique

Point examiné	Constat
Conditions d'utilisation et contrat lus (version, date)	
Contrat de sous-traitance (article 28 du RGPD) si des données personnelles peuvent être transmises	
Lieu d'hébergement, transferts hors de l'Union européenne et garanties	
Réutilisation des requêtes par l'éditeur pour améliorer ses modèles, et possibilité de la désactiver	
Conservation et effacement de l'historique	
Comptes professionnels, administration, double authentification, journalisation	
Droits demandés par l'outil et par ses connecteurs	

Inscription au registre des traitements, besoin d'une analyse d'impact	
Usage lié au recrutement ou à l'évaluation de salariés (article 6)	

Décision de la direction

☐ Accordée · ☐ Accordée sous conditions · ☐ Refusée. Niveau de données maximal : [] · réglages imposés : [] · date de réexamen : [] · motif en cas de refus : []

Nom et fonction	Date	Signature

Annexe E. Attestation de remise

Je soussigné(e) [nom, prénom], [fonction], reconnais avoir reçu la charte d'utilisation de l'intelligence artificielle générative de [raison sociale], version [1.0] du [date], et en avoir pris connaissance, ainsi que de l'information sur les contrôles et les traitements de données qui figure à son article 12. [J'ai suivi la sensibilisation prévue à l'article 11 le [date].]

Fait à	Le	Signature

Cette attestation prouve la remise de la charte et l'information de l'utilisateur. Elle n'en conditionne pas l'application, qui résulte des formalités rappelées dans le préambule. Un exemplaire est conservé par l'entreprise, un autre par l'utilisateur.