

LTC GROUP

AI • IT • SOFTWARE

L'IA, simplement.

Politique interne d'usage de l'intelligence artificielle

Usage responsable de l'IA au sein de LTC Group

En cohérence avec le RGPD et l'AI Act (art. 4 et 50)

Référence : LTC-IA-POL-001

Version : 1.0 **Date :** 22 juin 2026

Classification : Interne — opposable aux collaborateurs

Émetteur : LTC Group SRL

LTC Group SRL · Rue du Noir Jambon 13, 7830 Thoricourt, Belgique
BCE 1036.831.317 · TVA BE1036831317 · DUNS 374147096 · www.ltcai.be · contact@ltcai.be

Contrôle du document

Version	Date	Auteur / Validé par	Modifications	Revue
1.0	22/06/2026	Direction LTC Group	Création initiale	Annuelle

Statut

La présente politique est opposable à toute personne agissant pour le compte de LTC Group. Elle est portée à la connaissance des collaborateurs, qui en accusent réception (voir section Engagement).

Elle complète la Politique de protection des données (RGPD) et la Classification des risques AI Act. Les champs entre crochets [] sont à compléter. Elle est revue au minimum une fois par an et à chaque évolution réglementaire.

Sommaire

1. Objet et champ d'application

LTC Group utilise l'intelligence artificielle au quotidien, dans ses produits comme dans son fonctionnement interne. Cette politique fixe les règles d'un usage **responsable, sûr et conforme** de l'IA. Elle protège les données, le secret professionnel de nos clients, la qualité de nos livrables et notre réputation. Elle répond aussi à l'obligation de **maîtrise de l'IA** prévue par l'article 4 de l'AI Act.

À qui s'applique-t-elle ? À l'ensemble des cofondateurs, collaborateurs, stagiaires, indépendants et prestataires agissant pour le compte de LTC Group.

À quoi s'applique-t-elle ? À tous les outils d'IA utilisés en interne (assistants génératifs, copilotes, automatisations) ainsi qu'à l'usage de l'IA dans le cadre des produits LTC.

2. Les 5 règles d'or

#	Règle	Ce que cela signifie concrètement
1	L'humain garde la main	L'IA assiste, elle ne décide pas. Toute production est vérifiée et validée par une personne avant usage ou diffusion.
2	Confidentialité d'abord	On ne confie à un outil d'IA que des données autorisées. Jamais de données clients sensibles ou de secret professionnel dans un outil non couvert par un contrat.
3	Transparence	On indique l'usage de l'IA quand c'est pertinent, et on marque les contenus générés (voix, images, vidéos) diffusés.
4	Esprit critique	Une réponse d'IA n'est pas une vérité. On vérifie les faits, les chiffres et les sources avant de s'appuyer dessus.
5	Conformité et éthique	On respecte le RGPD, l'AI Act, la propriété intellectuelle et les valeurs de LTC Group : utile, honnête, au service du client.

3. Maîtrise de l'IA (« AI literacy » — art. 4 AI Act)

Depuis le 2 février 2025, l'AI Act impose d'assurer un niveau suffisant de compétence des personnes qui utilisent ou supervisent l'IA. LTC Group met en place :

- une sensibilisation à l'arrivée de chaque collaborateur (notions clés, risques, bonnes pratiques) ;
- une formation adaptée au rôle (utilisateur, développeur, supervision) ;
- une mise à jour régulière des connaissances en fonction des évolutions des outils et du cadre légal ;
- la mise à disposition de la présente politique et des documents de conformité associés.

4. Outils d'IA autorisés

Seuls les outils validés par la Direction peuvent être utilisés pour des tâches professionnelles. La liste ci-dessous est tenue à jour.

Outil	Usage approuvé	Conditions
Claude (Anthropic) — app & API	Assistance à la rédaction, à l'analyse, au code	Selon la classification des données ; pas d'entraînement

Outil	Usage approuvé	Conditions
		sur les données (API)
Microsoft Copilot	Productivité bureautique	Selon la classification des données
Outils LTC (Nota, Dedal IA, Demo Studio)	Usages métier	Dans le cadre défini pour chaque produit
ElevenLabs (Léa)	Synthèse vocale (produit)	Cadre produit + transparence « IA »
[Autres outils]	[À préciser]	[À valider par la Direction]

4.1 Demande d'un nouvel outil

Avant d'adopter un nouvel outil d'IA, le collaborateur sollicite la Direction / le référent IA. L'évaluation porte sur : la nature des données traitées, la localisation et les transferts, la politique d'entraînement du fournisseur, la sécurité et l'existence d'un contrat de sous-traitance (DPA) le cas échéant.

5. Quelles données peut-on confier à l'IA ?

Avant de saisir une information dans un outil d'IA, on identifie sa catégorie. La règle est simple : en cas de doute, on ne met pas.

Type de donnée	Outils approuvés (sous contrat)	Outils grand public non validés
Données publiques	Autorisé	Autorisé
Données internes non sensibles	Autorisé	À éviter
Données personnelles de clients / tiers	Autorisé si DPA + pseudonymisation	Interdit
Données notariales / secret professionnel	Uniquement via Nota + Veil™	Strictement interdit
Secrets, mots de passe, clés d'API	Interdit	Interdit

Règles absolues

Jamais de données clients sensibles ou de secret professionnel dans un outil d'IA grand public non couvert par un contrat.

Toujours pseudonymiser ou minimiser les données personnelles avant de les soumettre à un outil d'IA.

Jamais de mots de passe, clés d'API, identifiants ou secrets techniques dans une requête (« prompt »).

6. Supervision humaine et vérification

- Toute production de l'IA est relue et validée par une personne avant d'être utilisée ou diffusée ;
- Pour les sujets à fort enjeu (juridique, financier, médical, RH, sécurité), un double contrôle est appliqué ;
- Aucune décision produisant des effets significatifs pour une personne n'est prise sans intervention humaine ;

- On reste responsable de ce que l'on publie : l'IA ne dilue pas la responsabilité du collaborateur.

7. Transparence vis-à-vis des clients et des tiers

- On indique l'usage de l'IA lorsque c'est pertinent pour le client ou l'interlocuteur (en lien avec l'art. 50 de l'AI Act) ;
- Les agents conversationnels (ex. Léa) informent clairement qu'il s'agit d'une IA ;
- Les contenus synthétiques diffusés (voix, images, vidéos — ex. Demo Studio) sont marqués comme générés par IA ;
- On ne fait jamais passer une production d'IA pour le travail d'une personne identifiée sans son accord.

8. Usages strictement interdits

Sont interdits, sans exception :

- **Les pratiques prohibées par l'art. 5 de l'AI Act** : manipulation subliminale, exploitation de vulnérabilités, notation sociale, identification biométrique à distance en temps réel, et — dès le 2 décembre 2026 — la génération de contenus intimes non consentis ou de matériel d'abus sexuel d'enfants ;
- La saisie de données sensibles ou de secret professionnel dans un outil non autorisé ;
- La production de contenus trompeurs, diffamatoires, haineux ou illégaux ;
- La surveillance excessive des collaborateurs au moyen de l'IA ;
- Le contournement des mesures de sécurité ou des protections d'un système ;
- La violation de droits de propriété intellectuelle ou de droits d'auteur de tiers ;
- L'usage d'outils d'IA non validés pour des tâches impliquant des données professionnelles.

9. Qualité, biais et limites de l'IA

Les modèles d'IA peuvent produire des erreurs (« hallucinations »), reproduire des biais ou présenter des informations obsolètes. En conséquence :

- on ne présente jamais une sortie d'IA comme une vérité absolue ;
- on vérifie systématiquement les faits, chiffres, citations et références ;
- on reste attentif aux biais et on les signale ;
- on documente, pour les usages à enjeu, la vérification effectuée.

10. Sécurité

- Comptes nominatifs et authentification forte (MFA) ; pas de partage de comptes ;
- Pas d'installation d'extensions ou d'outils d'IA non validés sur les équipements professionnels ;
- Gestion sécurisée des clés d'API (jamais dans un prompt, un dépôt public ou un message) ;
- Respect des règles de sécurité décrites dans la Politique de protection des données.

11. Propriété intellectuelle et droits d'auteur

- On respecte les droits des tiers : pas de reproduction d'œuvres protégées via l'IA ;
- On vérifie que les contenus générés n'enfreignent pas de droits existants ;
- La titularité des contenus produits pour LTC Group est clarifiée et conservée par la Société, sauf accord contraire ;
- On cite les sources lorsque cela est requis.

12. Rôles, responsabilités et journalisation

Acteur	Responsabilité
Direction	Définit la politique, valide les outils, arbitre les cas particuliers.
Référent IA / DPD	Conseille, forme, instruit les demandes d'outils, traite les incidents.
Collaborateurs & prestataires	Appliquent la politique, vérifient les productions, signalent tout incident ou doute.

Les usages sensibles de l'IA sont tracés de manière proportionnée, afin de pouvoir rendre compte de la conformité.

13. Gestion des incidents

Tout incident lié à l'IA — fuite de données, sortie problématique, comportement inattendu d'un système, usage non conforme — est signalé **sans délai** au référent IA / DPD (admin@ltcai.be). Les incidents touchant des données personnelles suivent la procédure de gestion des violations de la Politique de protection des données.

14. Non-respect

Le non-respect de la présente politique peut entraîner des mesures disciplinaires ou contractuelles proportionnées, sans préjudice des conséquences légales (RGPD, AI Act) et des éventuelles responsabilités civiles ou pénales.

15. Engagement du collaborateur

Je reconnais avoir pris connaissance de la Politique interne d'usage de l'intelligence artificielle de LTC Group et m'engage à la respecter.

Nom et prénom	Fonction	Date et signature

16. Entrée en vigueur et révision

La présente politique entre en vigueur à sa date de validation. Elle est revue au minimum une fois par an, ainsi qu'à chaque évolution réglementaire (notamment de l'AI Act), changement d'outils ou à la suite d'un incident.

17. Documents liés

- Politique de protection des données (RGPD) — LTC Group ;
- Classification des risques AI Act — LTC Group ;
- **AIPD / DPIA — Plateforme Nota.**

Document établi par LTC Group SRL — « L'IA, simplement. »