CARBON

POLITIQUE D'UTILISATION RESPONSABLE DE L'INTELLIGENCE ARTIFICIELLE

OBJECTIFS DE LA POLITIQUE

La Politique d'utilisation responsable de l'IA (ci-après « **Politique** ») a pour objectif de définir les garanties, mesures et principes appropriés pour l'utilisation de l'intelligence artificielle (ci-après « **IA** ») chez CARBON SA, dont le siège est établi à 6000 Charleroi, Quai Arthur Rimbaud 6, immatriculée à la Banque Carrefour des Entreprises sous le numéro 0427.908.867 (RPM Hainaut, division Charleroi) (ci-après « **CARBON** »).

Cette Politique vise non seulement à assurer votre sécurité, vos intérêts et votre vie privée, mais également à garantir la sécurité, les intérêts et le respect des valeurs de CARBON, tout en veillant au respect des exigences légales et réglementaires.

La présente Politique s'inscrit notamment dans le respect :

- du Règlement (UE) 2024/1689 établissant des règles harmonisées concernant l'intelligence artificielle (« AI Act ») ;
- du Règlement (UE) 2016/679 (« RGPD ») ;
- de la législation belge applicable en matière de protection des données, de non-discrimination et de droit du travail

La présente Politique s'applique à tous les membres du personnel, consultants, sous-traitants, travailleurs/travailleuses temporaires, stagiaires et autres parties prenantes de CARBON (ci-après « **Utilisateur** ») qui choisissent d'utiliser l'IA pendant la durée de leur travail ou de toute autre relation d'affaires avec CARBON. La Politique est pertinente pour tout Utilisateur qui interagit avec les systèmes d'IA ou les utilise, directement ou indirectement, dans ses opérations quotidiennes. Cela inclut les personnes impliquées dans la saisie des données, l'entraînement des modèles, les processus de prise de décision et l'interprétation des résultats générés par l'IA.

PORTÉE

En établissant des lignes directrices et des attentes claires concernant l'utilisation des technologies d'IA, la Politique vise à promouvoir des pratiques responsables qui s'alignent sur les valeurs et les objectifs de CARBON tout en atténuant les risques potentiels associés au déploiement de l'IA.

Par conséquent, vous devez avoir lu et compris la présente Politique et vous conformer strictement à toutes les directives et principes qui y sont énoncés. Le non-respect de la Politique peut entraîner des mesures disciplinaires.

CARBON

QU'EST-CE QUE L'IA ?

Avant de plonger dans les détails de la Politique, il est important de savoir ce que signifie l'IA. En règle générale, l'IA fait référence à un large éventail de systèmes informatiques développés en recueillant des informations à partir de données (c'est-à-dire les « données d'entraînement ») et conçus pour effectuer des tâches nécessitant une intelligence humaine. Ces tâches comprennent l'apprentissage à partir des données, la prise de décisions éclairées, la reconnaissance de modèles, la compréhension du langage naturel et la génération de contenu.

Les technologies d'IA générative représentent une avancée significative dans ce domaine, permettant la création de nouveaux contenus, tels que la génération de texte et la synthèse d'images, basés sur des modèles appris à partir de données existantes.

Vous trouverez ci-dessous une liste d'outils d'IA couramment utilisés sur le lieu de travail :

- Chatbots / IA générative : ChatGPT, Microsoft Copilot, Perplexity, Google Gemini, Google Bard, Claude
- Assistant de réunion : otter.ai, Zoom AI Workplace Companion, Fathom, Fireflies
- Assistants à la rédaction : Jasper, Wordtune, Grammarly ;
- Outils de traduction : Deepl, Google Translate

Sachez que les exemples mentionnés ci-dessus sont non exhaustifs, c'est-à-dire que la Politique s'applique à toutes les utilisations des outils d'IA par les Utilisateurs dans l'exercice de leurs fonctions professionnelles.

Au sens de la présente Politique, la notion de système d'IA doit être interprétée conformément à l'article 3 du Règlement (UE) 2024/1689.

RISQUES LIÉS À L'UTILISATION DE L'IA

Bien que l'IA offre des avantages significatifs, elle présente également divers risques qui doivent être gérés avec soin. Les principaux risques associés à l'utilisation de l'IA sont les suivants :

- **Protection de la vie privée, confidentialité et sécurité** :
    - Les systèmes d'IA traitent souvent des données personnelles ou sensibles, qui pourraient être utilisées à mauvais escient ou exposées par des violations ou des mesures de sécurité inadéquates.

    - Certains systèmes d'IA peuvent en outre avoir été entraînés sur des ensembles de données dont l'origine ou la base juridique ne sont pas toujours transparentes, ce qui peut soulever des questions relatives à la protection des données et aux droits de propriété intellectuelle

- *Exemple* : Le fait de résumer les données confidentielles des clients à l'aide d'un outil d'IA sans examiner ses paramètres de confidentialité pourrait entraîner le partage d'informations sensibles à l'externe.

- **Préjugés et discrimination** :
  - Les outils d'IA produisent leur contenu à partir des données qu'ils extraient ou qui sont fournies par le biais de bases de données existantes. Une telle collecte non réglementée de données en tant que telle peut présenter un risque que le contenu reflète ou perpétue les préjugés existant présent dans les données d'entraînement. De tels préjugés peuvent entraîner un traitement partial ou discriminatoire de groupes ciblés de personnes.

  - L'utilisation d'outils d'IA qui ne sont pas conformes aux directives et aux normes éthiques de CARBON en tant que tels, peut promouvoir une activité susceptible de refléter ou de perpétuer un tel biais, créant ainsi une atteinte à la réputation ainsi que des responsabilités juridiques pour CARBON et les Utilisateurs.

  - *Exemple* : L'utilisation d'une IA pour filtrer les CV des candidats et les hiérarchiser peut conduire le système à favoriser involontairement les candidats masculins par rapport aux candidats féminins.

- **Inexactitude :**
  - L'IA peut générer des informations incorrectes ou fabriquées, ce qui peut induire les Utilisateurs en erreur ou entraîner de mauvaises décisions. Les résultats des systèmes d'IA peuvent ne pas être fiables ou adaptés au contexte, par exemple en raison de données d'entraînement incomplètes ou non représentatives.

  - *Exemple* : Utilisation de ChatGPT pour résumer les directives récentes d'une organisation gouvernementale, mais le système produit de fausses informations en raison d'un dysfonctionnement.

- **Perte de surveillance et de responsabilisation humaines** :
  - Une dépendance excessive à l'égard de l'IA peut entraîner une réduction de l'implication humaine, ce qui rend plus difficile l'identification et la correction des erreurs ou la prévention d'une mauvaise prise de décision de la part du système.

  - Les algorithmes d'IA impliquent souvent plusieurs agents tout au long de leur cycle de vie, des programmeurs qui les créent aux organisations qui les utilisent, en passant par tous les autres. Avec autant de contributeurs, il peut être difficile de tenir quelqu'un responsable de ce qui ne va pas avec l'IA.

  - *Exemple* : L'automatisation des réponses du support client à l'aide de l'IA peut entraîner des problèmes non résolus si l'IA comprend mal la demande et que personne n'examine son résultat.

- **Questions éthiques et réglementaires** :
    - L'utilisation de l'IA peut involontairement enfreindre les principes éthiques ou ne pas respecter les lois et réglementations, telles que le RGPD ou la loi sur l'IA.

    - *Exemple* : Utilisation de l'IA dans les interactions avec les clients et la prise de décision sans divulguer l'implication de l'IA.

- **Risques liés à la propriété intellectuelle** :
    - Si l'IA est entraînée sur des données protégés par le droit d'auteur (images, œuvres d'art, articles, ...), elle peut enfreindre des droits d'auteur, des marques ou des brevets, ou produire des résultats qui soulèvent des questions sur la propriété et les droits.

    - *Exemple* : la création de contenu marketing à l'aide d'un outil d'IA peut entraîner une violation des droits d'auteur si l'IA intègre du matériel protégé à partir de ses données d'entraînement.

PRINCIPES GÉNÉRAUX DE L'UTILISATION RESPONSABLE DE L'IA

Tous les Utilisateurs utilisant des systèmes d'IA au sein de CARBON sont tenus de suivre les principes décrits ci-dessous. Ces principes sont conçus pour promouvoir l'utilisation éthique, transparente et efficace de l'IA, en veillant à ce que son déploiement soit conforme à nos valeurs, à nos objectifs organisationnels et à nos obligations réglementaires.

- **Pensée critique :** Les membres du personnel doivent garder un état d'esprit critique lorsqu'ils interprètent les résultats des systèmes d'IA, car ces outils peuvent produire des erreurs, des inexactitudes ou des résultats incomplets. Il est essentiel d'évaluer la crédibilité des résultats de l'IA dans le contexte de la tâche à accomplir et de croiser ses résultats avec des sources fiables.

  La vérification des faits est une étape obligatoire pour s'assurer que les décisions basées sur des informations générées par l'IA sont exactes.

- **Surveillance humaine :** Les systèmes d'IA sont conçus pour responsabiliser les humains, et non pour les remplacer. Des mécanismes de surveillance appropriés doivent être mis en place afin que les Utilisateurs puissent intervenir si nécessaire, notamment en révisant, modifiant ou annulant des décisions générées par l'IA qui ne sont pas conformes aux normes éthiques, organisationnelles ou juridiques.

- **Reconnaître la responsabilité :** L'utilisation de l'IA dans les processus décisionnels ne transfère pas la responsabilité à la technologie elle-même. Les Utilisateurs doivent comprendre que la responsabilité ultime de toute action ou décision éclairée par l'IA incombe à l'individu ou à l'équipe qui utilise le système.

CARBON interdit toute prise de décision produisant des effets juridiques ou affectant significativement une personne physique lorsqu'elle est fondée exclusivement sur un traitement automatisé, y compris le profilage, sauf si :

- une base légale appropriée existe ;
- une analyse juridique préalable a été réalisée ;
- une intervention humaine réelle et effective est garantie ;
- les droits des personnes concernées sont assurés (droit d'accès, de rectification, de contestation).

- **Se conformer aux lois :** les Utilisateurs doivent s'assurer que toute utilisation de l'IA est conforme aux cadres juridiques et réglementaires applicables, y compris, mais sans s'y limiter, la loi sur l'IA, le RGPD, les lois sur la propriété intellectuelle et d'autres réglementations sectorielles pertinentes. Non seulement le non-respect met en péril l'intégrité et la réputation de CARBON, mais il peut également entraîner des conséquences juridiques et financières importantes.

- **Transparence** : Soyez toujours transparent lorsque vous utilisez l'IA. Les Utilisateurs doivent divulguer quand l'IA a été utilisée pour générer du contenu, éclairer des décisions ou effectuer des tâches, en particulier dans des contextes où cela affecte les parties prenantes, les clients ou le public. Ne présentez jamais quelque chose comme votre propre travail lorsqu'il a été exclusivement ou partiellement réalisé par l'IA.

  Lorsque la loi l'exige (notamment en cas d'interaction avec des personnes physiques affectées par une décision), les personnes concernées doivent être informées de l'utilisation d'un système d'IA, conformément à l'AI Act et au RGPD.

- **Évitez de trop vous fier à l'IA** : utilisez l'IA comme un outil pour soutenir, et non remplacer, le jugement et l'expertise humains. Demandez-vous toujours si l'utilisation de l'IA apportera une valeur ajoutée à la tâche à accomplir.

- **Tenez compte de l'environnement :** les systèmes d'IA nécessitent souvent des ressources de calcul importantes, ce qui entraîne une consommation d'énergie élevée et une empreinte CARBON potentiellement importante. Les membres du personnel doivent tenir compte de cet impact environnemental en réservant l'utilisation de l'IA aux tâches où son application est réellement nécessaire ou offre des avantages substantiels. Par exemple, l'IA ne doit pas être utilisée pour des activités de moindres importances telles que la vérification orthographique de base ou la simple création de listes, car ces tâches peuvent être accomplies avec un minimum de ressources à l'aide d'outils traditionnels.

  CARBON encourage une utilisation proportionnée des outils d'IA, conciliant innovation, efficacité et réduction de l'impact environnemental des technologies numériques.

- **Anonymiser les données :** les Utilisateurs ne doivent jamais saisir d'informations personnelles, confidentielles ou relatives aux clients dans les systèmes d'IA, car ces

outils peuvent stocker, traiter ou partager ces données d'une manière qui pourrait enfreindre les lois sur la protection de la vie privée ou les accords de confidentialité. Même des données apparemment inoffensives peuvent présenter des risques si elles sont mal manipulées ou combinées à d'autres informations. En anonymisant les entrées ou en s'abstenant de partager complètement des données sensibles, les Utilisateurs peuvent minimiser le risque de violation de données, d'accès non autorisé ou d'utilisation non prévue des informations.

- **Identifier les biais** : les Utilisateurs doivent surveiller activement les signes de préjugés dans les sorties générées par l'IA, car les biais peuvent provenir d'algorithmes sous-jacents, de données d'entraînement ou d'interprétations erronées du contexte. Lorsqu'un biais est identifié, les Utilisateurs sont responsables de faire remonter le problème à l'équipe appropriée.

- **Suivre le manuel d'instructions** : Les Utilisateurs doivent respecter strictement les instructions, les directives et les meilleures pratiques fournies par les développeurs ou les fournisseurs du système d'IA (le cas échéant). Cela inclut la compréhension de l'utilisation prévue, des limites et des risques potentiels du système. En suivant ces instructions, les Utilisateurs peuvent éviter une utilisation abusive ou des conséquences involontaires qui pourraient exposer la responsabilité de CARBON ou nuire à sa réputation.

- **Inclusion et équité :** Les Utilisateurs veillent à utiliser les systèmes d'IA de manière à promouvoir un traitement équitable des personnes, à prévenir les discriminations et à favoriser des décisions respectueuses de la diversité et de l'inclusion. Toute utilisation susceptible d'entraîner une discrimination directe ou indirecte doit être évitée et signalée.

CAS D'UTILISATION DE L'IA À HAUT RISQUE

Certaines utilisations de l'IA présentent un risque élevé pour la santé, la sécurité ou les droits fondamentaux. Ces systèmes sont soumis à des obligations de conformité strictes.

Sont considérés comme "Haut Risque" au sein de CARBON, notamment :

- **Ressources Humaines (Recrutement & Gestion) :** Outils utilisés pour le tri automatique de CV, l'évaluation des candidats, la prise de décision sur les promotions ou la résiliation des contrats de travail.

- **Notation de Crédit et Évaluation des Risques (Investissement) :** L'utilisation d'IA pour évaluer la solvabilité de personnes physiques (ex : entrepreneurs et entrepreneuses, garants et garantes) ou établir leur notation de crédit.

Obligations pour les utilisateurs de systèmes "Haut Risque"

Les Utilisateurs souhaitant utiliser ou déployer un tel système doivent impérativement respecter les mesures suivantes (art. 26 AI Act) :

- **Supervision Humaine :** Garantir qu'une personne physique compétente et formée a le dernier mot sur toute décision automatisée ("Human in the loop").
- **Analyse d'Impact (AIPD) :** Réaliser une Analyse d'Impact relative à la Protection des Données (DPIA) avant toute mise en production. Avant tout déploiement d'un système d'IA à Haut Risque, une évaluation de conformité contractuelle et technique du fournisseur doit être réalisée (documentation CE, marquage, obligations AI Act).
- **Qualité des Données :** S'assurer que les données d'entrée sont pertinentes et représentatives pour éviter les biais discriminatoires.
- **Journalisation (Logs) :** Les journaux d'activité doivent être conservés pendant une durée proportionnée aux finalités poursuivies et en cohérence avec la politique IT et la réglementation applicable, avec un minimum indicatif de six (6) mois ;
- **Transparence :** Informer clairement les personnes concernées (personnes candidates, porteurs et porteuses de projet) qu'elles font l'objet d'une analyse par un système d'IA.

En raison des risques de sanctions lourdes, l'utilisation de tout système d'IA à Haut Risque requiert **l'autorisation écrite et préalable** du Délégué à la Gestion Journalière.

PRATIQUES INTERDITES ET USAGES PROSCRITS

Conformément à la réglementation en vigueur, CARBON s'interdit de développer, de déployer ou d'utiliser des systèmes d'Intelligence Artificielle relevant des catégories suivantes :

A. Manipulation et atteinte à l'autonomie

- Tout système utilisant des techniques subliminales ou délibérément manipulatrices visant à altérer le comportement d'une personne de manière à lui causer un préjudice physique ou psychologique.
- Tout système exploitant les vulnérabilités spécifiques d'individus ou de groupes (liées à l'âge, au handicap ou à la situation économique).

B. Surveillance et classification sociale

- Le recours au "social scoring" (notation sociale) consistant à évaluer la fiabilité d'une personne physique sur la base de son comportement social, conduisant à un traitement défavorable dans d'autres contextes.
- La création ou l'alimentation de bases de données de reconnaissance faciale par extraction massive et non ciblée (scraping) d'images provenant d'internet ou de réseaux de vidéosurveillance.

C. Analyse biométrique et comportementale

- L'utilisation de systèmes d'IA pour inférer les émotions des collaborateurs sur le lieu de travail ou des apprenants dans les cadres de formation, sauf cas de sécurité critique dûment justifié.
- La catégorisation biométrique des individus sur la base de données sensibles (race, opinions politiques, convictions religieuses, orientation sexuelle, etc.).
- L'utilisation d'IA de police prédictive basée uniquement sur le profilage de personnalité pour évaluer le risque de commission d'infractions.

D. Identification en temps réel

- L'usage de systèmes d'identification biométrique à distance "en temps réel" dans les espaces accessibles au public est strictement interdit, sauf dans les limites dérogatoires prévues par la loi et après autorisation d'une autorité administrative ou judiciaire compétente.

FORMATION

CARBON s'engage à ce que tous les Utilisateurs soient pleinement conscients des comportements responsables à adopter en utilisant l'IA et des risques et limitations associés.

Une formation est organisée régulièrement et adaptée au niveau de risque des fonctions concernée

SURVEILLANCE ET APPLICATION DE LA LOI

CARBON s'assure que la Politique est respectée et correctement mise en œuvre. Tous les Utilisateurs qui se servent des outils d'IA dans l'exercice de leurs fonctions chez CARBON doivent se conformer à la présente Politique.

En cas de violation, des mesures disciplinaires appropriées peuvent être prises.

NOTIFICATION D'UNE VIOLATION

CARBON attend de tous les Utilisateurs des outils d'IA qu'ils soient attentifs à la détection des événements qui pourraient indiquer une violation de la présente Politique. Si vous avez connaissance d'une telle violation par un autre Utilisateur ou un tiers, vous êtes tenu d'en informer votre supérieur hiérarchique dans les plus brefs délais. Les informations suivantes doivent être communiquées en même temps que la notification :

(i) les données qui ont été compromises ;
(ii) quel outil IA a été utilisé pour commettre la violation ;
(iii) la date à laquelle la violation a été commise ; et
(iv) les parties concernées.

CARBON s'assure que l'identité du rapporteur reste confidentielle à tout moment.

EXAMEN DE LA POLITIQUE

La Politique sera révisée chaque année ou au besoin pour tenir compte de l'évolution des risques liés à l'IA, des changements réglementaires et des progrès technologiques.

ENTRÉE EN VIGUEUR

La présente Politique entre en vigueur à compter du 1er mars 2026

Fait à Charleroi le 19 octobre 2026

_____

Grégoire Dupuis
Délégué à la gestion journalière

Champ d'application	CARBON SA
Entrée en vigueur	1/03/2026
Modifications	19/10/2026
Diffusion	Par e-mail à l'ensemble des membres du personnel et accessible dans le fichier interne suivant : P:\Politique du Groupe.