RETRAITE COMPLEMENTAIRE
agirc-arrco

GSIT
Note de sécurité

LIMITATION DE L'USAGE DES INTELLIGENCES ARTIFICIELLES GÉNÉRATIVES

Objet : Ce document est une note de sécurité sur l'émergence des solutions d'intelligences artificielles génératives et de leur utilisation au sein de l'Agirc-Arrco

Diffusion : [Interne]
L'émetteur est le seul à diffuser le document aux personnes concernées : Restreinte *La diffusion est limitée au GIE Agirc-Arrco : Interne*

Version	Date	Objet	Auteur(s)	Etat
1.1	25/09/2023	Compléments et validation	GSIT	**Validé par :** **RSSI : N. DELOUCHE** **DRCP : L. AIT ALI SLIMANE** **DTI : L. POULALION**

Historique des versions

1.0		Rédaction initiale	GSIT	

AGIRC-ARRCO

Note de sécurité

Version 1.1

SOMMAIRE

Note de sécurité

Version 1.1

1 Objet, destinataires, contexte

Ce document a pour objet de définir l'état de l'art et les limites d'utilisation de solutions d'intelligence artificielle génératives au sein de l'Agirc-Arrco.

La note s'adresse à l'ensemble des utilisateurs des SI de l'Agirc-Arrco, quels que soient leur rôle et fonction.

À l'instar du précurseur et médiatique « Chat GPT », les acteurs du numériques mettent à disposition du grand public des outils basés sur l'Intelligence Artificielle (IA), capables de générer et d'éditer du contenu de différents types en répondant aux diverses requêtes des utilisateurs, appelés **IA Générative**. Ces solutions, du fait de leur performance et leur facilité d'utilisation, vont impacter rapidement les usages professionnels. Il convient d'avoir conscience des risques associés à leur usage et d'en encadrer les pratiques.

La DSI-RC est consciente que ces IA Générative présentent un intérêt certain et a engagé une réflexion afin de permettre la mise à disposition d'usages encadrés et sécurisés d'IA Génératives. Dans l'attente de cette mise à disposition ce qui suit s'applique à tous.

2 Risques

1) Les données sont exposées de façon non maîtrisée par conséquent il ne faut pas qu'elles puissent être reliées à l'Agirc Arrco.
2) Les plateformes d'IA agrègent des données préexistantes mais également celles soumises par les utilisateurs ; toute requête est sauvegardée et exploitée par la plateforme. L'effacement n'est pas forcément maîtrisé, par exemple pour ChatGPT l'utilisateur doit effectuer l'action d'effacement manuellement.
3) Les résultats proviennent de sources non vérifiées, potentiellement manipulés, il convient donc d'interpréter avec précaution les résultats produits.

Dans le cadre de l'Agirc Arrco, les mesures suivantes sont destinées à maîtriser les risques ci-dessus.

3 Mesures de maîtrise et règles d'usage

3.1 Anonymisation des comptes et requêtes

Il est interdit de créer un compte ChatGPT, ou autre, avec une adresse mail **@agirc-arrco.fr**

Si vous aviez déjà créé un compte ChatGPT, ou autre, avec votre adresse mail Agirc-Arrco **il convient sans tarder d'effacer les conversations puis le résilier.**

Il est interdit de transmettre dans une conversation ChatGPT, ou autres, des éléments de configuration technique non anonymisés, des extraits de code source AA, des données métier ou autres données non publiques.

En particulier **ne pas transmettre** celles concernant :

- Les technologies et versions utilisées au sein de l'Agirc-Arrco (base de données, middleware, …)
- Des informations d'accès, d'identité (type et nomenclature de compte, les solutions utilisées, …)
- Des informations à caractères personnelles
- Des informations concernant l'activité de l'entreprise (contrats, …)
- Des informations RH (CV, etc…)
- Du code informatique contenant des informations propres à l'Agirc Arrco

Il est interdit de contextualiser les requêtes avec le nom Agirc-Arrco, celui des partenaires ou d'autres régimes.

3.2 Stockage et effacement des requêtes et de leur résultat

À ce jour, il n'y a aucune garantie sur les modalités de collecte, de stockage et d'utilisation des données transmises à des tiers. Il faut donc faire attention à ce qui est renseigné dans les requêtes.

Après une utilisation dans le cadre professionnel il est demandé d'effacer manuellement les requêtes et leur résultat.

3.3 Qualité de l'information fournie

Le résultat fourni par ces plateformes dépend entièrement de la façon dont le moteur IA détermine les mots les plus probables en fonction de la qualité de la requête exprimée. Par ailleurs, la plateforme se source sur les publications internet, contrôlées ou non, de sources fiables ou manipulées.

Si les résultats proposés sont parfois d'une très grande qualité, il ne faut pas accepter ces réponses sans un minimum d'esprit critique, de recul et de contrôle.

Une précaution toute particulière devra être appliquée en cas de recherche d'une solution à un problème de configuration technique par exemple.

Ces plateformes n'apportent aucune garantie quant à la pertinence ou la validité de la réponse.

3.4 Propriété intellectuelle

Les plateformes utilisant et agrégeant des données existantes, aucune garantie de respect de la propriété intellectuelle n'est apportée. Utiliser tout ou partie d'un résultat peut exposer à un usage illicite.