Note

Émetteur(s) :	Centre d'Excellence SAP - Pôle France
Destinataire(s) :	L'ensemble des collaborateurs SAP du Pôle France
Copie(s) :	
Objet :	**Note information utilisation revue code ChatGPT**

1. Introduction

Nous constatons que des requêtes de demande d'analyses et de génération de code (ABAP ou Fiori) sont réalisées notamment via l'utilisation de l'intelligence artificielle ChatGPT.

Cette note a pour objectif de vous donner la position actuelle du Centre d'Excellence SAP du Pôle France sur l'usage d'outil d'IA pour la génération/optimisation de code (Envoi ou réception de code source sur application tierce sur la zone internet).

2. Qu'est-ce que ChatGPT ?

https://fr.wikipedia.org/wiki/ChatGPT

« ChatGPT est un prototype d'agent conversationnel lancé en novembre 2022 par OpenAI, une société co-créée par Elon Musk

ChatGPT est un prototype d'agent conversationnel utilisant l'intelligence artificielle, développé par OpenAI et spécialisé dans le dialogue. L'agent conversationnel est un modèle de langage affiné par apprentissage supervisé et par apprentissage par renforcement.

Lancé en novembre 2022 dans une version non connectée à Internet, ChatGPT bénéfice d'une large exposition médiatique et reçoit un accueil globalement positif, bien que son exactitude factuelle soit critiquée.

En raison de ses capacités multiples, le prototype suscite également des inquiétudes en raison des détournements possibles à des fins malveillantes, des risques de plagiat dans le monde académique et de possibles suppressions d'emplois dans certains secteurs. »

ChatGPT est donc un service basé sur du Machine Learning* hébergé à l'étranger auquel vous envoyez des données (instructions et/ou code applicatif) pour obtenir un résultat.

* Machine Learning : Tout ce qui peut être stocké numériquement peut servir de données pour le Machine Learning. En décelant les patterns dans ces données, les algorithmes apprennent et améliorent leurs performances dans l'exécution d'une tâche spécifique.

3. Quels sont les risques ?

Extrait des conditions de ChatGPT (https://openai.com/terms/) :

"You may provide input to the Services ("Input"), and receive output generated and returned by the Services based on the Input ("Output"). Input and Output are collectively "Content." As between the parties and to the extent permitted by applicable law, you own all Input, and subject to your compliance with these Terms, OpenAI hereby assigns to you all its right, title and interest in and to Output. OpenAI may use Content as necessary to provide and maintain the Services, comply with applicable law, and enforce our policies. You are responsible for Content, including for ensuring that it does not violate any applicable law or these Terms."

Extrait des "Privacy" de ChatGPT (https://openai.com/privacy/) :

Category of Personal Information	Sources of Personal Information	Use of Personal Information	Disclosure of Personal Information
Social Information	We may collect Social Information from you when you interact with our Social Media Pages.	We may use Social Information to perform analytics and to communicate with you.	We may disclose Social Information to our affiliates.
Communication Information	We collect Communication Information directly from you.	We use Communication Information for providing our Services and responding to you.	We disclose Communication Information to our affiliates and communication services providers.
Technical Information	We collect Technical Information from you.	We use Technical Information for analytics and in some cases, for moderation and prevention of fraud and malicious activity by users of our Services.	We disclose Technical Information to our affiliates and analytics provider(s).

En résumé : Vous consentez à ce que votre code soit stocké et utilisé par OpenAI et/ou ses partenaires.

Les fuites de code source sont l'un des plus grands risques auxquels sont confrontés les développeurs de logiciels aujourd'hui. Il expose les secrets commerciaux sensibles, la propriété intellectuelle et les secrets commerciaux. Cela expose également le code source lui-même au risque d'être utilisé à des fins malveillantes.

Lorsque le code source fuit, cela peut entraîner un certain nombre de problèmes. Par exemple, cela pourrait permettre aux pirates de voler une adresse IP. Cela pourrait exposer des informations sensibles sur les clients. Cela pourrait exposer les employés au risque de se faire voler leur identité. Et cela pourrait causer des problèmes juridiques aux entreprises.

En effet, selon une récente étude menée par KPMG, près de la moitié des personnes interrogées ont déclaré avoir subi une fuite d'informations confidentielles ou propriétaires. Parmi ceux-ci, près des deux tiers ont déclaré que la fuite était due au départ d'un développeur de l'entreprise.

4. Conclusion

A ce stade et au vu des connaissances actuelles et de la position de nos clients, il est formellement interdit d'utiliser ces outils d'IA dite générative ChatGPT ou Github Copilot (liste non exhaustive).