**Annexe Intelligence Artificielle**

**Prestation de support, d’évolution et de pilotage du Service Desk de France Travail**

**SIAO2505**

**Annexe – Système d’IA et Destination**

Description du Système d’IA :

Le système d’IA souhaité par France Travail doit permettre d’alimenter les réponses d’un Chatbot et d’un VoiceBot en language naturel sur la Base d’articles de connaissance de France Travail sur l’environnement de travail.

D’autres bases de connaissance pourront à terme alimenter ce système d’IA.

Le système d’IA doit également permettre de l’automatisation dans l’aide à la création d’articles de connaissance sur la base de réponses d’expert.

Destination :

Le système d’IA souhaité doit servir à apporter des réponses, et dans certains cas, des résolutions aux sollicitations de tous les agents France Travail et de ses partenaires ayant un accès au système d’information de France Travail en termes de support sur l’environnement de travail.

**Annexe – Jeux de données**

Les jeux de données mise à disposition par France Travail sont basés sur nos bases de connaissances, ainsi qu’un jeux de donnée provenant de l’historique des incidents de l’utilisateur

* Jeux de données de France Travail

Les Jeux de données suivants sont transmis au Titulaire par France Travail au titre du Contrat ou doivent être créés ou collectés au titre du Contrat.

|  |  |
| --- | --- |
| **Description du Jeu de données** | **Obligation de détruire le Jeu de données à l’expiration du terme du Contrat** |
| Base de connaissance FT | Oui |
| Historique des incidents de l’utilisateur | Oui |

* Jeux de données du Titulaire et Jeux de données des tiers

Les Jeux de données du Titulaire et Jeux de données des tiers suivants seront ou ont été utilisés pour l’entraînement (le cas échéant) et la validation du Système d’IA et les essais auxquels il est soumis:

|  |  |  |
| --- | --- | --- |
| **Réponse du soumissionnaire** | | |
| **Description du Jeu de données** | **Droits d’utilisation de France Travail** | **Obligation de transmettre le Jeu de données à l’expiration du terme du Contrat** |
|  |  | Oui/Non |
|  |  | Oui/Non |
|  |  | Oui/Non |
|  |  | Oui/Non |

**Annexe – Mesures visant à garantir la transparence**

*Le soumissionnaire fournit en tant que futur titulaire ici une description des mesures techniques et organisationnelles qu’il prend pour assurer la transparence dans le cadre du système d’IA.*

|  |
| --- |
| **Réponse du soumissionnaire** |
|  |

**Annexe –Mesures visant à garantir la surveillance humaine.**

*Le soumissionnaire en tant que futur titulaire fournit ici une description des mesures techniques et organisationnelles qu’il prend pour assurer la surveillance humaine dans le cadre du système d’IA.*

|  |
| --- |
| **Réponse du soumissionnaire** |
|  |

**Annexe – Niveaux d’exactitude**

*Le soumissionnaire en tant que futur titulaire décrit ici les niveaux requis d’exactitude dans le cadre du système d’IA.*

|  |
| --- |
| **Réponse du soumissionnaire** |
|  |

**Annexe – Mesures pour garantir un niveau approprié de robustesse, de sécurité et de cybersécurité**

*Le soumissionnaire en tant que futur titulaire fournit une description des mesures techniques et organisationnelles qu’il prend pour garantir un niveau approprié de robustesse, de sécurité et de cybersécurité dans le cadre du système d’IA.*

*Ces mesures doivent garantir que le système d’IA soit aussi résilient que possible face aux erreurs, défauts ou incohérences qui peuvent survenir au sein du système ou de l’environnement dans lequel le système fonctionne, notamment en raison de l’interaction avec des personnes physiques ou d’autres systèmes.*

*Le Système d’IA résiste aux tentatives de tiers non autorisés visant à modifier son utilisation, son comportement, ses résultats ou ses performances en exploitant les vulnérabilités du système.*

*Les solutions techniques destinées à remédier aux vulnérabilités spécifiques à l’IA peuvent comprendre, le cas échéant, des mesures ayant pour but de prévenir, de détecter, de contrer, de résoudre et de maîtriser les attaques visant à manipuler le Jeu de données d’entraînement («empoisonnement des données»), ou les composants pré-entraînés utilisés pour l’entraînement («empoisonnement des modèles»), les données d’entrée destinées à induire le modèle en erreur («exemples adverses» ou «exfiltration de modèles»), les attaques contre la confidentialité ou les défauts du modèle, qui peuvent conduire à la prise de décisions préjudiciables.*

|  |
| --- |
| **Réponse du soumissionnaire** |
|  |