MINISTÈRE
DE L'ACTION
ET DES COMPTES
PUBLICS

Liberté
Égalité
Fraternité

CHARTE D'UTILISATION DE L'IA AU CISIRH

MINISTÈRE
DE L'ACTION
ET DES COMPTES
PUBLICS
Liberté
Égalité
Fraternité

Données sensibles - Définition

Qu'est-ce qu'une donnée sensible ?

« Les informations sensibles sont les informations dont la divulgation à des personnes non autorisées, l'altération ou l'indisponibilité sont de nature à porter atteinte à la réalisation des objectifs des entités qui les mettent en œuvre. Les systèmes qui les traitent font l'objet de mesures de sécurité renforcées, définies selon les principes de l'II 901, sous réserve des réglementations spécifiques applicables. », ***Arrêté du 13 décembre 2023 portant approbation de la politique ministérielle de sécurité numérique des ministères économiques et financiers***

Exemples

- ✓ Une donnée à caractère personnel
- ✓ Les informations correspondant à un secret couvert par la loi
- ✓ Une information technique
- ✓ Un document interne au CISIRH
- ✓ Le Noyau n'est pas une donnée sensible

MINISTÈRE
DE L'ACTION
ET DES COMPTES
PUBLICS
Liberté
Égalité
Fraternité

Règles d'usage de l'IA – Généralités

- ✓ La doctrine IA de l'Etat s'impose au CISIRH, à ses agents et à ses prestataires (lien à venir)
- ✓ Le RGPD et l'IA Act continuent de s'appliquer à tous nos usages.
- ✓ Seul les outils autorisés et/ou homologués par le CISIRH peuvent être utilisés pour des usages professionnels.
- ✓ **Ne pas fournir de données sensibles** (données à caractère personnel, documents de l'Etat ou du CISIRH, informations sur le fonctionnement interne du CISIRH, etc.) **SAUF avec des LLM qualifiés SECNUMCLOUD dans un système homologué par le CISIRH. L'usage de données sensibles doit alors être restreint aux seules données nécessaires à l'usage.**
- ✓ **L'activation de la recherche Web avec des données sensibles est interdit.**
- ✓ L'usage automatisé de systèmes d'IA pour des actions critiques sur le SI est interdit (cf. doctrine IA de l'Etat n°2)
- ✓ Responsabilité : l'utilisateur reste responsable de l'usage qu'il fait des données fournies par l'IA (ex : si une donnée erronée conduit à un dysfonctionnement des systèmes du CISIRH) et doit systématiquement en contrôler les résultats.
- ✓ Les utilisateurs de systèmes d'IA doivent veiller à un usage durable : minimisation des tokens, choix de modèles adaptés à la tâche demandée, non dépendance aux modèles, garder une capacité à se passer de l'IA, non détérioration des conditions de travail…

MINISTÈRE
DE L'ACTION
ET DES COMPTES
PUBLICS
Liberté
Égalité
Fraternité

Les systèmes d'IA au sein du CISIRH

Systèmes d'IA homologués par le CISIRH

Le CISIRH a souscrit auprès de la société Jamespot des licences à l'application Safebrain. Cette application est hébergée chez Outscale en SecNumcloud. Il convient de distinguer 2 types de modèles de langages (LLM) :

- *LLM SecNumCloud = permet le traitement des données personnelles / confidentielles.*
- *LLM non SecNumcloud = autorisés pour les autres traitements.*

Autres systèmes d'IA autorisés par le CISIRH (homologués par la DINUM)

ALBERT API = au centre de la doctrine IA de l'Etat pour la puissance de calcul, ALBERT API est la cible d'usage pour les traitements au sein des SI du CISIRH (ex : CREP à partir d'un transcript d'entretien) ou des développeurs.

L'Assistant IA = issu d'un partenariat entre l'IA et Mistral, il s'agit d'un Chatbot à usage individuel.

Systèmes d'IA interdits par le CISIRH pour des usages professionnels

Les IA « grand public » (Chat GPT, Gemini…), y compris avec un abonnement personnel ou emprunté.

Les IA professionnelles avec un abonnement personnel ou emprunté.

⇒ Ces cas constituent une situation d'illégalité d'usage pour le CISIRH et les utilisateurs

⇒ Des systèmes d'IA spécifiques pourront être souscrits après validation du besoin par la Direction du CISIRH, une analyse par le RSSI et la précision des règles d'usage qui s'y appliqueront.

MINISTÈRE
DE L'ACTION
ET DES COMPTES
PUBLICS
Liberté
Égalité
Fraternité

Cas d'usage : IA générative documentaire

Assistance à l'édition / création de document ou de texte, directement ou via un corpus documentaire

- ✓ **Les données et documents de confidentialité « C1 – Non protégé » peuvent être utilisés avec tous les LLM.**
- ✓ **Les données et documents de confidentialité « C2 – Confidentiel » doivent obligatoirement être traités avec un système IA SecNumCloud.**
- ✓ **Il est interdit d'utiliser des données ou documents de confidentialité « C3 – Restreint », y compris sur les systèmes IA actuellement à disposition des agents / prestataires du CICIRH.**
- ✓ Il convient de s'assurer de ne pas porter atteinte à des droits de propriété intellectuelle
- ✓ La technologie RAG augmente la qualité des réponses mais n'est pas parfaite et le LLM reste fortement dépendant de son corpus d'entrainement, ce qui impacte ses réponses.
- ✓ Il est nécessaire de ne pas prendre de décision fondée uniquement sur le résultat généré. Il convient de vérifier les informations fournies par le système d'IA.

MINISTÈRE
DE L'ACTION
ET DES COMPTES
PUBLICS
Liberté
Égalité
Fraternité

Cas d'usage : Développement logiciel assisté par IA

Règles de bases du CISIRH

- ✓ Le code source généré par IA doit faire l'objet de mesures de contrôle afin de vérifier son innocuité et sa conformité aux normes d'accessibilité portées par le RGAA
  - ✓ Passage obligatoire dans SonarQube
  - ✓ Ne pas autoriser le commit automatique
  - ✓ S'assurer que le code source est contrôlé par un humain avant son intégration (responsabilité du responsable technique du projet)
- ✓ La génération de code source est interdite pour les briques critiques, notamment :
  - ✓ les modules de cryptographie (authentification, chiffrement, signature, etc.)
  - ✓ les modules de gestion des droits d'accès des utilisateurs et administrateurs
- ✓ Sensibilisation obligatoire et dédiée des développeurs
- ✓ La doctrine IA de l'Etat n°2 s'impose aux développeurs (internes et prestataires) (lien à venir)