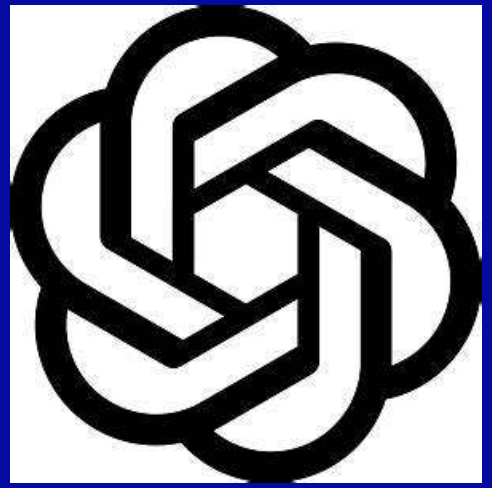
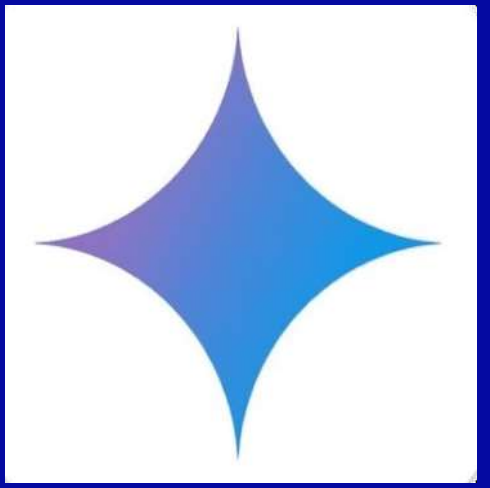
Confidentialité des données

Alliance de l'industrie touristique du Québec

Principes de cybersécurité et bonnes pratiques

ChatGPT, Copilot, Gemini : les LLMs et la confidentialité

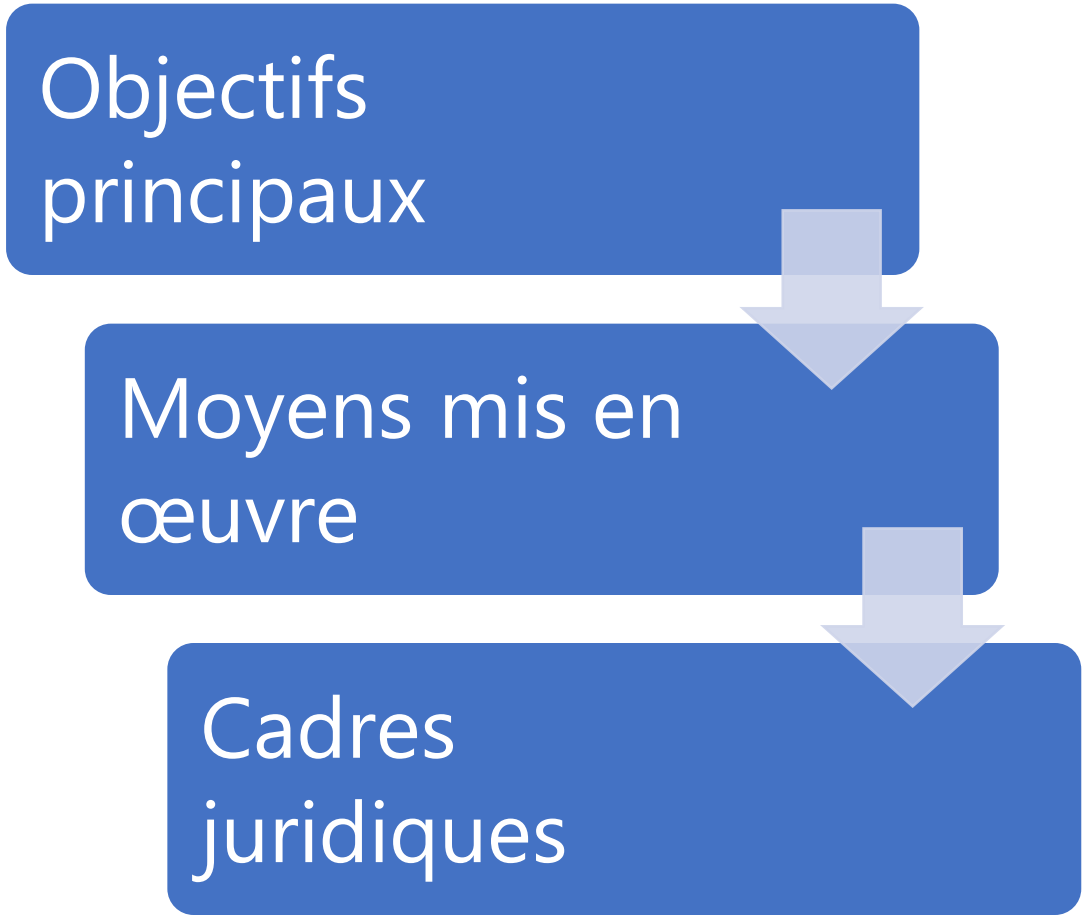




Confidentialité des données

La confidentialité des données désigne le principe et l'ensemble des pratiques visant à protéger les informations personnelles ou sensibles contre l'accès, l'utilisation ou la divulgation non autorisés.

Elle s'inscrit dans une démarche plus large de **sécurité de l'information** et de **protection de la vie privée**.



Moyens mis en œuvre

- Contrôle d’accès
- Chiffrement des données en transit ou repos
- Politique internes de gestion des données
- Formations et sensibilisation des employés
- Audits et surveillance

Cadres juridiques

- Le RGPD (Règlement Général sur la Protection des Données)
- La Loi sur la protection des renseignements personnels
- Le HIPAA pour les données de santé aux États-Unis

Les LLMs et la confidentialité

Version gratuite (grand public) :

•Les données **peuvent être utilisées pour entraîner les modèles**.

•Stockage temporaire sur les serveurs.

•Option pour désactiver l'utilisation des données via les **paramètres de confidentialité**.

Team / Enterprise (usage professionnel) *:*

•**Zéro utilisation des données client** pour l'entraînement.

•Chiffrement des données **en transit (TLS)** et **au repos (AES-256)**.

•Conformité : **SOC 2, ISO 27001, GDPR**.

•Les administrateurs peuvent **contrôler l'accès** et gérer les permissions.

•Adaptation à l'utilisation sans entrainement

Bonnes pratiques pour l’utilisation sécuritaire

- Contrôlez les informations partagées
- Ne transmettez jamais de données personnelles, financières, médicales ou confidentielles non nécessaires.
- Analysez les documents avant téléversement pour repérer les éléments sensibles.
- Préférez l’anonymisation des contenus
- Remplacez noms, identifiants, numéros de dossier ou adresses par des alias ou données génériques avant l’analyse.
- Sensibilisez votre équipe
- Mettez en place une courte formation ou une note de service expliquant l’usage responsable de l’IA générative.
- Clarifiez les risques et les obligations internes liés à la confidentialité.