



T-LAW

Compta Companion

Etude de faisabilité légale

Sommaire

- 1. Introduction**
 - 1.1. Contexte du projet**
 - 1.2. Objectifs de l'étude**
 - 1.3. Méthodologie de l'étude**
- 2. Cadre Juridique**
 - 2.1. Réglementation applicable à la gestion des données personnelles**
 - **RGPD (Règlement Général sur la Protection des Données)**
 - **Législations équivalentes à l'international**
 - **Loi Informatique et Libertés**
 - 2.2. Responsabilité liée à l'utilisation d'un LLM**
 - 2.3. Règles spécifiques aux professions comptables et financière**
- 3. Analyse des Risques Légaux**
 - 3.1. Sécurité des données**
 - 3.2. Conformité au droit des contrats et responsabilité des utilisateurs**
 - 3.3. Propriété intellectuelle**
- 4. Contraintes Techniques et Légales**
 - 4.1. Hébergement des données**
 - 4.2. Transparence et applicabilité**
 - 4.3. Archivage et traçabilité**
 - 4.4. Conformité fiscale et comptable**
- 5. Modèle de Gouvernance et Recommandations Légales**
 - 5.1. Mise en place d'une gouvernance des données**
 - 5.2. Charte éthique et légale**
 - 5.3. Mise en conformité continue**
- 6. Conclusion et Plan d'Action**
 - 6.1. Synthèse des principaux défis juridiques**
 - 6.2. Étapes clés pour garantir la faisabilité légale**
 - 6.3. Recommandations finales**

1. Introduction

1.1. Contexte du projet

L'application en cours de conception vise à offrir un service d'analyse et de conseil en finance et comptabilité basé sur un Large Language Model (LLM). Les utilisateurs pourront déposer des documents financiers (fiches de paie, devis, factures, etc.) sur la plateforme, qui seront traités par l'IA. L'objectif est de permettre des interactions dynamiques où les utilisateurs peuvent poser des questions financières et comptables précises basées sur leurs documents.

1.2. Objectifs de l'étude

Cette étude vise à évaluer la faisabilité légale de cette application, en identifiant les risques et contraintes juridiques et en proposant des solutions pour assurer la conformité réglementaire.

1.3. Méthodologie de l'étude

- Analyse des lois et réglementations pertinentes (RGPD, normes comptables, IA Act, etc.)
- Identification des risques juridiques et des obligations légales
- Propositions de mesures correctives et préventives

2. Cadre Juridique

2.1. Réglementation applicable à la gestion des données personnelles

a. RGPD (Règlement Général sur la Protection des Données)

- Les documents financiers contiennent des données à caractère personnel (ex. : noms, salaires, adresses). Ils relèvent des catégories de données sensibles, imposant des obligations accrues en matière de sécurité et de consentement.
- Obligations principales :
 - Obtenir un consentement explicite et informé des utilisateurs.

- Assurer la portabilité, la rectification ou la suppression des données à leur demande.
- Mise en place de mesures de sécurité telles que le chiffrement des données.
- Articles clés :
 - Article 6 : Base légale pour le traitement des données.
 - Article 7 : Consentement clair et explicite.
 - Article 25 : Principe de "Privacy by Design" et "Privacy by Default".
 - Article 32 : Sécurité des données.
 - Article 35 : Réalisation d'une Analyse d'Impact sur la Protection des Données (DPIA) pour les traitements à haut risque.

b. Législations équivalentes à l'international

- Conformité à des normes similaires (CCPA aux États-Unis, PIPL en Chine) en cas d'utilisation par des utilisateurs hors UE.

c. Loi Informatique et Libertés (modifiée par le RGPD)

- Articles 34 et 35 : Obligation de sécurité des données personnelles.

2.2. Responsabilité liée à l'utilisation d'un LLM

- **Fiabilité des réponses** : Le LLM peut fournir des interprétations ou des analyses erronées des données, exposant l'application à des litiges pour information trompeuse.
- **Clause limitative de responsabilité** : Les CGU doivent stipuler que les réponses fournies sont à titre informatif et ne substituent pas un avis professionnel.
- **Obligation d'applicabilité** : Fournir des justifications claires des réponses générées par l'IA.
- Articles clés :
 - Code civil français, Article 1240 : Responsabilité civile délictuelle (dommages causés par des erreurs du service).
 - Code de la consommation, Article L121-3 : Obligation d'information claire et non trompeuse pour les consommateurs.
 - Directive européenne sur le commerce électronique (transposée en France), Articles 6 et 7 : Obligation de mention légale et de transparence.

2.3. Règles spécifiques aux professions comptables et financières

- Respect des normes comptables locales et internationales (IFRS, GAAP, etc.).
- Conformité aux obligations des experts-comptables et des conseillers financiers en matière d'éthique et de secret professionnel.
- Articles clés :
 - Ordonnance 45-2138 du 19 septembre 1945 : Réservé à des professionnels certifiés la validation ou l'émission d'avis en matière comptable ou fiscale.
 - Directive DAC6 : Signalements pour certaines pratiques fiscales transfrontalières.

3. Analyse des Risques Légaux

3.1. Sécurité des données

- **Risque de violation de données** : En cas de fuite, des informations sensibles peuvent être compromises.
- **Mesures recommandées** :
 - Stockage des données dans des environnements conformes (éventuellement certifiés ISO 27001).
 - Mise en place d'une stratégie de chiffrement des données au repos et en transit.
 - Surveillance continue pour détecter les tentatives de cyberattaques.
- Articles clés :
 - RGPD, Article 32 : Sécurité des traitements de données.
 - Loi Informatique et Libertés, Article 34 : Obligation de garantir la confidentialité des données.
 - Décret n° 2018-137 : Obligations en matière de cybersécurité.

3.2. Conformité au droit des contrats et responsabilité des utilisateurs

- **Conditions Générales d'Utilisation (CGU)** :
 - Clauses sur la propriété intellectuelle des données fournies par les utilisateurs.
 - Déclaration des limitations liées à l'usage des conseils générés.
 - Garantie de respect des droits des tiers (ex. : si l'utilisateur dépose un document qu'il ne possède pas légalement).

3.2. Propriété intellectuelle

- **Contenus générés par le LLM** : Clarifier les droits de propriété intellectuelle sur les réponses produites.
- **Utilisation de documents soumis** : Définir des clauses garantissant que les données fournies ne sont pas exploitées à des fins secondaires.
- Articles clés :
 - Code de la propriété intellectuelle, Article L111-1 : L'utilisateur conserve les droits d'auteur sur les documents qu'il télécharge.
 - Articles L122-4 et L335-3 : Prohibition de l'utilisation non autorisée de documents tiers.
 - RGPD, Article 20 : Droit à la portabilité des données.

4. Contraintes Techniques et Légales

4.1. Hébergement des données

- **Localisation géographique des serveurs** :
 - Privilégier l'UE pour bénéficier d'un cadre RGPD strict.
 - Garantir la conformité des prestataires cloud (AWS, Azure, Google Cloud) avec les normes internationales.

4.2. Transparence et applicabilité

- **Obligations en matière d'IA** :
 - Conformité à l'éventuel futur IA Act en Europe : mise en place d'un audit de l'algorithme pour identifier les biais.
 - Explications claires des limites du modèle (réponses statistiques et non expertes).

4.3. Archivage et traçabilité

- Conservation des interactions utilisateur pour des raisons juridiques.
- Mise en place d'un système d'audit trail pour tracer les événements majeurs dans la gestion des données.

4.4. Conformité fiscale et comptable

- Articles clés :
 - Code général des impôts (CGI), Articles L102 B à L102 F : Conservation et traitement des données fiscales.
 - Code de commerce, articles L123-12 à L123-23 : Obligation de tenue de comptabilité conforme.

5. Modèle de Gouvernance et Recommandations Légales

5.1. Mise en place d'une gouvernance des données

- **Rôles et responsabilités :**
 - Identification d'un DPO pour assurer la conformité au RGPD.
 - Définition des procédures internes pour traiter les incidents de sécurité.

5.2. Charte éthique et légale

- Intégration d'une charte pour encadrer les engagements de l'application vis-à-vis des utilisateurs.
- Proposition d'une communication transparente des mécanismes de collecte, traitement et usage des données.

5.3. Mise en conformité continue

- **Audits réguliers :**
 - Tests de conformité RGPD.
 - Contrôle des biais dans les réponses du LLM.
- **Veille juridique :**
 - Surveillance des évolutions réglementaires liées à l'IA et à la protection des données.

6. Conclusion et Plan d'Action

6.1. Synthèse des principaux défis juridiques

- Risques de non-conformité au RGPD.
- Responsabilités liées aux conseils financiers automatisés.
- Sécurité et propriété intellectuelle des données traitées.

6.2. Étapes clés pour garantir la faisabilité légale

- Implémentation des mesures de sécurité et de conformité RGPD.
- Adoption d'un cadre contractuel clair pour les utilisateurs.
- Réalisation d'audits préventifs sur l'IA.

6.3. Recommandations finales

- Renforcer la transparence vis-à-vis des utilisateurs.

- Prévoir une assistance humaine pour compléter les réponses IA sur des cas complexes.
- Définir des politiques de gouvernance solides pour anticiper les risques futurs.

Cette étude fournit un cadre détaillé pour assurer la conformité et minimiser les risques juridiques de l'application tout en favorisant son développement.