Voici le rapport de conformité du document « IA - Procédure de conformité v.0.6.2 - Dicte.ia », mis à jour pour inclure une analyse basée sur la nouvelle grille d'évaluation fournie.

Ce rapport évalue la conformité du projet Dicte.ia en se basant sur les réponses fournies dans le questionnaire (IA - Procédure de conformité v.0.6.2 - Dicte.ia.pdf) et en les analysant à travers le prisme des critères et des recommandations de la grille d'évaluation (IA - Procédure de conformité - Grille d'évaluation v.1.pdf), tout en se référant directement au RGPD et au RIA.

**Rapport d’Analyse de Conformité (v2)**

**Projet :** Utilisation de l'outil Dicte.ia pour l'enregistrement, la retranscription automatisée et le compte-rendu de réunion (CSA). **Documents de référence :**

* IA - Procédure de conformité v.0.6.2 - Dicte.ia (Questionnaire)
* IA - Procédure de conformité - Grille d'évaluation v.1 (Grille d'évaluation)
* Règlement (UE) 2016/679 (RGPD)
* Règlement (UE) 2024/1689 (RIA)

**1. Description du projet et réglementations applicables**

**1.1. Contexte et applicabilité du RIA**

Le projet est destiné à un usage en **gestion administrative** par les services académiques. Il ne relève pas de la recherche ou du développement scientifique.

* **Évaluation :** Le RIA est applicable.

**1.2. Qualification de l'outil : IA ou algorithme simple**

Le questionnaire indique que l'outil utilise "un ou des systèmes à base d’IA". La définition d'un système d'IA comme un "système automatisé qui est conçu pour fonctionner à différents niveaux d’autonomie" et qui peut générer des sorties comme du contenu correspond à l'outil Dicte.ia.

* **Évaluation :** Le projet implique l'utilisation d'une IA. La procédure de conformité IA doit donc se poursuivre.

**1.3. Pratiques interdites en matière d'IA (Article 5 du RIA)**

La finalité du projet est la retranscription et le compte-rendu de réunions. Sur la base de cette description, le projet ne semble pas relever des pratiques interdites par l'article 5 du RIA, telles que la manipulation, la notation sociale ou l'utilisation de données biométriques pour la catégorisation de personnes sur la base de données sensibles.

* **Évaluation :** Le projet **ne paraît pas constituer une pratique interdite**.

**1.4. Finalités et prise de décision automatisée**

Les finalités du traitement ("Enregistrement, retranscription automatisée et compte-rendu de réunion") paraissent **déterminées, explicites et légitimes**, conformément à l'article 5.1.b du RGPD. Le questionnaire indique que l'utilisation de l'outil **ne conduit pas à une prise de décision** concernant des agents ou usagers.

* **Évaluation :** Le projet **ne paraît pas impliquer de prise de décision automatisée** produisant des effets juridiques ou similaires (Article 22 du RGPD).

**1.5. Autres réglementations applicables**

D'après la grille d'évaluation, plusieurs autres référentiels et réglementations s'appliquent potentiellement :

* **[SI DE L’ETAT]** : Le projet, en collectant et traitant des données pour les missions des services de l'État (rectorat), fait partie du système d'information de l'État.
* **[PSSIE]** : La Politique de Sécurité des Systèmes d’Information de l’État s'applique à tous les SI des administrations de l'État.
* **[SECURITE CNIL]** : Ce guide s'applique dès lors qu'il y a un traitement de données personnelles.
* **[CLOUD AU CENTRE]** et **[SECNUMCLOUD]** : L'hébergement est de type Cloud Computing. Les données traitées incluent des données de santé et des opinions politiques/syndicales, qui peuvent être considérées comme des "données d'une sensibilité particulière". Par conséquent, la doctrine "Cloud au Centre" et le référentiel SecNumCloud sont applicables.
* **Évaluation :** Des travaux de conformité supplémentaires sont nécessaires pour ces réglementations.

**2. Conformité au RGPD**

**2.1. Traitement de données à caractère personnel**

Le questionnaire confirme que le projet engendre un traitement de données à caractère personnel. Les données incluent :

* **Données d'identification** (nom, prénom, enregistrement sonore).
* **Données de vie professionnelle** (profession, employeur).
* **Données sensibles (catégories particulières de l'article 9 du RGPD)** : santé, biométrie, opinions politiques, philosophiques, convictions religieuses ou appartenance syndicale.
* **Évaluation :** Le projet engendre un traitement sur des données à caractère personnel et le RGPD s'applique intégralement. Le traitement de données sensibles doit être pris en compte pour l'analyse des risques.

**2.2. Statut des acteurs et responsabilités**

* **Selon le RIA :** Le porteur de projet (service académique) utilise une "offre commerciale [...] clé en main" développée par un acteur externe (Dicte.ia). Il est donc un **déployeur** au sens du RIA.
* **Selon le RGPD :** Le porteur de projet détermine les finalités et les moyens du traitement (enregistrer et retranscrire les CSA). Il est donc **responsable du traitement**. Le prestataire Dicte.ia traite les données pour le compte du responsable du traitement ; il est donc **sous-traitant**.
* **Évaluation :**
  + Porteur de projet : Déployeur et Responsable du traitement.
  + Prestataire (Dicte.ia) : Fournisseur et Sous-traitant.
* **Recommandation :** La relation avec le prestataire externe nécessite un acte juridique contraignant, un **contrat de sous-traitance conforme à l'article 28 du RGPD**. Or, le questionnaire indique que la contractualisation est incertaine ("Je ne sais pas").

**2.3. Base légale et licéité du traitement**

Le questionnaire n'indique **aucune base légale** pour le traitement (consentement, obligation légale, contrat, etc.). Le traitement de données sensibles (santé, opinions politiques/syndicales) est interdit par principe (Article 9.1 du RGPD), sauf dérogations strictes (ex: consentement explicite).

* **Évaluation :** Le traitement **n'apparaît pas correctement fondé juridiquement**.
* **Recommandation :** Il est impératif de revoir la détermination de la base légale avec le porteur de projet. Pour les données sensibles, le consentement explicite des personnes concernées est probablement la seule base légale envisageable.

**2.4. Privacy by Design et obligations générales**

La notice de la grille d'évaluation rappelle que certains points essentiels de conformité RGPD ne sont pas traités par le questionnaire (registre, transparence, droits des personnes, minimisation, conservation, sécurité) mais restent des obligations pour le responsable de traitement.

* **Registre des traitements :** Le traitement **n'est pas référencé** dans le registre du rectorat, ce qui contrevient à l'article 30 du RGPD.
* **Transferts de données hors UE :** Le prestataire Dicte.ia est français, mais le **lieu (pays) de traitement des données est inconnu**. La nationalité française du prestataire ne garantit pas que les données ne sont pas traitées hors UE, notamment en cas de recours à des sous-traitants ultérieurs.
  + **Évaluation :** Il est impossible de déterminer s'il y a un transfert hors UE. Un risque d'extraterritorialité d'un droit étranger ne peut être exclu.
  + **Recommandation :** Il est crucial d'identifier les lieux de traitement et, en cas de transfert hors UE, de s'assurer de l'existence d'une décision d'adéquation ou de garanties appropriées (ex: CCT).
* **Analyse d'Impact relative à la Protection des Données (AIPD) :**
  + Critères cochés : "Collecte de données sensibles ou données à caractère hautement personnel" et "Usage innovant ou application de nouvelles solutions technologiques ou organisationnelles".
  + **Évaluation :** Avec **deux critères remplis**, la réalisation d'une AIPD **doit être menée** avant la mise en œuvre du traitement, conformément à l'article 35 du RGPD.

**3. Conformité au RIA**

**3.1. Classification du système d'IA**

* **Est-ce un système à haut risque ?**
  + Le système n'est pas un composant de sécurité d'un produit listé à l'Annexe I du RIA.
  + Il faut vérifier l'Annexe III. Le projet ne correspond à aucune des finalités listées (biométrie, infrastructures critiques, éducation, emploi, services essentiels, répression, migration, justice).
  + Le système ne semble pas non plus remplir les conditions d'exception (tâche procédurale étroite, amélioration d'une activité humaine, etc.).
  + **Évaluation :** Le projet **ne constitue pas un système d'IA à haut risque**.
* **Est-ce un modèle d'IA à usage général ?** L'outil Dicte.ia semble spécialisé dans la retranscription et ne présente pas la "généralité significative" d'un modèle capable d'exécuter "un large éventail de tâches distinctes".
  + **Évaluation :** Le projet **ne constitue pas un modèle d'IA à usage général**.
* **Le projet implique-t-il une obligation de transparence ?**
  + Le système **génère du contenu de synthèse** (texte : retranscription, compte-rendu).
  + **Évaluation :** Le projet **constitue un système d'IA impliquant une obligation de transparence** selon l'article 50 du RIA.

**3.2. Respect des obligations de transparence (Article 50 RIA)**

Le questionnaire de conformité (section 5.4) n'a pas été rempli car les obligations n'entreront en vigueur qu'en 2026. Cependant, l'analyse révèle des non-conformités futures si le projet est maintenu en l'état.

* **Obligations du fournisseur (Dicte.ia) :** Les contenus générés (texte) devront être **marqués comme ayant été générés par une IA**, via une solution efficace et fiable.
* **Obligations du déployeur (service académique) :** Si les textes générés sont publiés pour informer le public sur des questions d'intérêt public, ils devront indiquer qu'ils ont été manipulés par une IA, sauf en cas de contrôle humain ou éditorial effectif.
* **Évaluation actuelle :** Le questionnaire ne prévoit aucune mesure d'information.
* **Évaluation future :** L'information relative au système d'IA **devra être prévue/revue** pour être conforme.

**4. Synthèse et Recommandations**

Le projet Dicte.ia présente des **non-conformités critiques et multiples avec le RGPD**. Sur le plan du RIA, bien que le système ne soit pas classé à haut risque, il ne respecte pas les futures obligations de transparence.

|  |  |  |  |
| --- | --- | --- | --- |
| **Point de Contrôle** | **Conformité RGPD** | **Conformité RIA** | **Recommandations Urgentes** |
| **Base légale du traitement** | 🔴 **Non Conforme** | N/A | **Définir et documenter une base légale valide**, notamment le **consentement explicite** pour le traitement des données sensibles. |
| **Analyse d'Impact (AIPD)** | 🔴 **Non Conforme** | N/A | **Réaliser une AIPD** avant toute mise en œuvre en raison des risques élevés (données sensibles, nouvelle technologie). |
| **Relations avec le sous-traitant** | 🔴 **Non Conforme** | N/A | **Signer un contrat de sous-traitance** conforme à l'article 28 du RGPD avec le prestataire Dicte.ia. |
| **Transfert de données hors UE** | 🔴 **Non Conforme** | N/A | **Clarifier le lieu de traitement des données** et s'assurer que des garanties suffisantes sont en place si un transfert hors UE est identifié. |
| **Inscription au registre** | 🔴 **Non Conforme** | N/A | **Inscrire le traitement au registre** des activités de traitement du rectorat. |
| **Transparence (RIA)** | N/A | 🔴 **Non Conforme (à l'avenir)** | **Prévoir des mesures pour marquer** les contenus générés comme étant issus d'une IA, conformément à l'article 50 du RIA. |
| **Sécurité (Cloud)** | 🔴 **Non Conforme** | N/A | Le traitement de données sensibles via un service Cloud impose le **respect de la doctrine "Cloud au Centre" et potentiellement la qualification SecNumCloud**. |

**Conclusion générale :**

Le déploiement du projet Dicte.ia est **fortement déconseillé en l'état**. Les manquements aux principes fondamentaux du RGPD (licéité, transparence, responsabilité) exposent le responsable de traitement à des risques juridiques et de sécurité importants.

**Il est impératif de suspendre le projet et de ne le réévaluer qu'après la mise en œuvre complète des recommandations RGPD, en particulier la définition d'une base légale valide et la réalisation d'une AIPD.**