

Analyse des risques de conformité RGPD et IA

Introduction	2
Diagnostic Global : Un Projet en Rupture avec les Principes Fondamentaux du RGPD	3
Analyse Détaillée des Risques par Fonctionnalité Critique	4
Fonctionnalité : Analyse biométrique et physiologique	4
Fonctionnalité : Profilage multidimensionnel sensible	4
Fonctionnalité : Suivi familial et traitement des données de mineurs	4
Fonctionnalité : Recommandation adaptive cross-profil	5
Synthèse et Recommandation : Nécessité d'une Révision Stratégique Impérative	6
Non-conformité par Conception ("By Design")	6
Risques IA non maîtrisés	6
Insuffisance des Mesures Correctrices	6
Recommandation Formelle	6

Introduction

Cette note a pour objet de présenter à la direction une synthèse des risques juridiques et éthiques critiques identifiés suite à l'analyse des cahiers des charges du projet. L'analyse révèle des non-conformités systémiques au Règlement Général sur la Protection des Données (RGPD) et des dangers significatifs liés à l'usage de l'intelligence artificielle. Ces constats ne révèlent pas des faiblesses à corriger, mais une incompatibilité fondamentale entre la vision actuelle du projet et le cadre légal, rendant une révision stratégique immédiate non pas optionnelle, mais impérative.

Diagnostic Global : Un Projet en Rupture avec les Principes Fondamentaux du RGPD

L'analyse croisée du cahier des charges, du registre des traitements et de la matrice des risques révèle que la majorité des fonctionnalités proposées contreviennent directement aux principes fondamentaux de la protection des données. Ces manquements ne sont pas marginaux mais structurels, exposant l'entreprise à des risques juridiques et réputationnels maximaux.

Plusieurs violations systémiques des principes du RGPD ont été identifiées de manière récurrente dans les documents de projet :

- Absence de base légale valide (Art. 6 & 9) : Des traitements critiques, comme l'analyse biométrique ou le profilage sensible, sont envisagés sans base légale appropriée. Le Registre de traitements qualifie explicitement le traitement des données de santé et biométriques d'« illégal » et le profilage sensible d'« illicite », confirmant l'absence de toute base légale viable.
- Violation du principe de minimisation et de limitation de la conservation (Art. 5) : La fonctionnalité "Inscription à vie" constitue une violation directe de l'obligation de limiter la durée de conservation des données et entre en conflit direct avec le droit à l'effacement.
- Manquement à l'obligation de transparence et d'information (Art. 13 & 14) : Les décisions entièrement automatisées et opaques, telles que celles du module de recommandation, privent les utilisateurs de l'information sur la logique sous-jacente des traitements qui les concernent.
- Prise de décision automatisée sans garanties (Art. 22) : Des fonctionnalités comme le "Traitement automatisé des exclusions" et la "Recommandation adaptive cross-profil" instaurent des décisions produisant des effets significatifs sans intervention humaine ni possibilité de recours, ce qui est formellement interdit.

Ces manquements systémiques se matérialisent de manière particulièrement critique dans plusieurs fonctionnalités phares du projet, qui sont détaillées ci-après.

Analyse Détaillée des Risques par Fonctionnalité Critique

L'analyse suivante se concentre sur les fonctionnalités présentant les niveaux de risque les plus élevés, qualifiés de "Critique" avec une priorité d'action "Immédiate". Pour chaque cas, nous mettons en évidence la nature des violations RGPD, les risques éthiques liés à l'IA, et les conséquences directes pour les personnes concernées.

Fonctionnalité : Analyse biométrique et physiologique

Ce module vise à réaliser un suivi morphologique évolutif des clients à partir de photos, vidéos et données de santé.

Type de Risque Description de la Non-Conformité et du Danger Violations RGPD Traitement de données de santé et biométriques sans base légale (Art. 9), absence de minimisation (Art. 5), et obligation de réaliser une AIPD non respectée. Le registre qualifie ce traitement d'« illégal ». Risques IA & Éthiques L'explicabilité du modèle est jugée « très difficile ». Le risque de discrimination basée sur la santé ou le physique est qualifié de « Maximal ». Impact sur les personnes Discrimination santé/physique, Surveillance de masse, Atteinte à la dignité, et Stigmatisation.

En l'état, cette fonctionnalité constitue une violation délibérée de l'article 9 du RGPD, la rendant non seulement illégale mais également indéfendable devant une autorité de contrôle.

Fonctionnalité : Profilage multidimensionnel sensible

L'objectif est d'extraire des signaux religieux, idéologiques, politiques et sentimentaux à partir des données partagées par les utilisateurs, notamment depuis leurs réseaux sociaux.

Type de Risque Description de la Non-Conformité et du Danger Violations RGPD Traitement de données sensibles (Art. 9), absence de base légale (Art. 6), et décision automatisée sans garantie (Art. 22). Le registre juge ce profilage « illicite ». Risques IA & Éthiques Risques élevés de biais algorithmique, de profilage opaque et d'inférences abusives, nécessitant un « Contrôle humain obligatoire ». Impact sur les personnes Discrimination liées à la religion/opinion, Manipulation, Atteinte à la liberté de pensée/expression, et exclusion sociale.

Ce traitement expose l'entreprise à des sanctions maximales pour exploitation illicite de données sensibles et crée un risque réputationnel majeur de manipulation et de discrimination.

Fonctionnalité : Suivi familial et traitement des données de mineurs

Ce module propose d'associer les achats aux différents membres du foyer, y compris les enfants, afin de construire un historique des besoins de la famille sur plusieurs années.

Type de Risque Description de la Non-Conformité et du Danger Violations RGPD Absence de consentement parental pour les mineurs (Art. 8) et absence de base légale pour les membres de

la famille (Art. 6). Le registre qualifie le traitement des données de tiers/mineurs de « NON CONFORME ». Risques IA & Éthiques Risque de profilage comportemental des familles et des mineurs et d'inférences non consenties sur les habitudes domestiques ou parentales. Impact sur les personnes Profilage d'enfants, Surveillance de la famille, Atteinte à la vie privée, et Traçabilité des mineurs non consentants.

Le profilage non consenti de mineurs est une ligne rouge réglementaire et éthique, rendant cette fonctionnalité inacceptable et dangereuse dans sa conception actuelle.

Fonctionnalité : Recommandation adaptive cross-profil

L'objectif est d'adapter les recommandations en continu en détectant des événements de vie majeurs comme un divorce, un déménagement ou un changement de carrière.

Type de Risque Description de la Non-Conformité et du Danger Violations RGPD Décision entièrement automatisée produisant des effets significatifs sans garanties (Art. 22), et manquement à l'obligation d'information sur la logique sous-jacente (Art. 13 & 15). La matrice souligne la nécessité d'une « Intervention humaine obligatoire ». Risques IA & Éthiques Risques critiques de prédictions intrusives, de manipulation comportementale et d'inférences cross-profil sans contrôle de l'utilisateur. Impact sur les personnes Manipulation de la vie privée, Prédiction intrusive, Absence de contrôle sur les recommandations, et Influence sans consentement.

Cette approche proactive, bien que commercialement attractive, crée une surveillance intrusive qui anéantit la confiance de l'utilisateur et contrevient directement aux interdictions relatives à la prise de décision automatisée.

La nature et la gravité des risques identifiés dans ces fonctionnalités clés démontrent l'incompatibilité du cahier des charges actuel avec un cadre légal et éthique responsable.

Synthèse et Recommandation : Nécessité d'une Révision Stratégique Impérative

L'analyse détaillée confirme que les problèmes ne peuvent être résolus par de simples ajustements techniques. La conception même de nombreuses fonctionnalités repose sur des prémisses illégales et éthiquement intenable, ce qui impose une réorientation fondamentale de la stratégie produit, et non de simples ajustements techniques.

Non-conformité par Conception ("By Design")

Des fonctionnalités comme l'analyse biométrique, le profilage sensible et l'"inscription à vie" sont intrinsèquement non conformes au RGPD. Leur mise en œuvre exposerait l'entreprise à des sanctions maximales et à une interdiction de traitement, un risque existentiel pour le service.

Risques IA non maîtrisés

L'usage de l'IA pour des décisions automatisées critiques (exclusions, recommandations basées sur des événements de vie) est envisagé sans les garanties indispensables de supervision humaine, d'explicabilité et d'audit des biais, créant un risque "Critique" de discrimination et de manipulation.

Insuffisance des Mesures Correctrices

Les "mesures correctrices" listées (ex: "Obtenir le consentement", "Réaliser une AIPD") sont nécessaires mais insuffisantes pour valider des finalités de traitement qui sont, à la base, excessives ou illicites. Plusieurs fonctionnalités nécessitent une action radicale de type "Supprimer" ou "Arrêt du traitement".

Recommandation Formelle

Au vu de la gravité et du caractère systémique des risques, nous recommandons l'arrêt immédiat des développements basés sur le cahier des charges actuel et le lancement d'une phase de révision stratégique du projet.

Cette révision doit avoir pour objectif de redéfinir les fonctionnalités pour qu'elles soient alignées, dès leur conception, sur les principes de "Privacy by Design", de minimisation des données et d'éthique de l'IA.

Cette réorientation n'est pas seulement une obligation de conformité, mais une condition essentielle pour bâtir un service digne de confiance et durable.