Plan d'Action de Mise en Conformité RGPD & IA Act

Introduction et Contexte Stratégique

Introduction

Ce document constitue une feuille de route opérationnelle et priorisée, visant à mettre le projet en conformité avec les exigences du Règlement Général sur la Protection des Données (RGPD) et les dispositions émergentes de l'EU AI Act. Basé sur l'analyse approfondie des risques et l'état des registres de traitements fournis, les actions décrites ci-après sont impératives pour garantir la viabilité juridique, la robustesse éthique et la pérennité commerciale du projet.

Synthèse des Risques Majeurs

L'analyse des documents sources a mis en évidence plusieurs risques critiques qui compromettent la légalité et la sécurité du projet. Ces risques, s'ils ne sont pas traités immédiatement, exposent l'organisation à des sanctions maximales et à une perte de confiance irréversible. Les principaux points de non-conformité sont :

- **Traitement illégal de données sensibles** : La collecte et l'analyse de données biométriques, de santé, religieuses et politiques sont actuellement effectuées sans aucune base légale valide, en violation directe de l'Article 9 du RGPD.
- **Manque de base légale valide** : De multiples traitements, incluant le suivi familial et l'envoi de produits, sont opérés sans le consentement approprié des personnes concernées, y compris des tiers et des mineurs.
- **Décisions entièrement automatisées à impact significatif** : Des fonctionnalités de recommandation et de profilage prennent des décisions intrusives (par exemple, suite à un divorce) sans la supervision humaine et les garanties exigées par l'Article 22 du RGPD.
- **Conservation illimitée des données** : Le concept d'inscription "à vie" contrevient frontalement au principe de limitation de la durée de conservation et au droit à l'effacement (droit à l'oubli).
- **Risques de biais et de discrimination** : Les systèmes d'IA, en l'absence de gouvernance et d'audits, présentent un risque élevé de générer des profilages opaques, des biais discriminatoires et des inférences abusives.

Équipes Concernées et Rôles

Ce plan d'action est destiné aux équipes **Juridique**, **Produit**, et **Technique**. Chaque action identifie clairement les principaux acteurs responsables de sa mise en œuvre, afin d'assurer une coordination efficace et une prise de responsabilité claire.

Chantier Prioritaire 1 : Analyse biométrique et physiologique

Analyse Stratégique : Contexte et Risques

La fonctionnalité d'analyse biométrique est un axe de personnalisation stratégique, mais telle qu'elle est implémentée, elle n'est pas simplement "à haut risque" ; elle est fondamentalement illégale au regard de l'Article 9 du RGPD. Sa poursuite sous cette forme expose l'entreprise à des amendes réglementaires maximales et à un effondrement réputationnel immédiat. Les actions qui suivent ne sont pas des optimisations mais des prérequis impératifs à toute opération légale de cette fonctionnalité.

Diagnostic de Non-Conformité

Violations et Risques Identifiés	Criticité / Priorité
Violations RGPD : Art. 9 (traitement de données sensibles), Art. 6 (absence de base légale), Art. 5 (minimisation).	Criticité : Critique Priorité : Immédiate
Risques pour les personnes : Discrimination basée sur la santé ou le physique, surveillance de masse, atteinte à la dignité, perte de contrôle sur des données intimes.	Criticité : Critique Priorité : Immédiate

Plan d'Action Correctif

Les actions suivantes sont obligatoires et doivent être mises en œuvre avant toute mise en production de la fonctionnalité.

1. **Obtention d'une Base Légale Valide (Juridique, Produit)** : Implémenter un mécanisme de **consentement explicite**, spécifique et éclairé (conformément à l'Art. 9.2.a du RGPD) qui doit être recueilli *avant* toute collecte de photos, vidéos ou données de santé.
2. **Interdiction du Croisement avec des Données Publiques (Juridique, Tech)** : **Supprimer le croisement avec les banques d'images publiques**. Cette pratique de traitement ultérieur est illicite et doit être stoppée, sauf à obtenir un consentement distinct, spécifique et explicite pour cette finalité précise.
3. **Réalisation d'une Analyse d'Impact (Juridique, Tech)** : Mener et documenter une **Analyse d'Impact relative à la Protection des Données (AIPD) complète** pour identifier, évaluer et mitiger les risques. La CNIL devra être consultée si des risques résiduels élevés persistent (Art. 36).

4. **Minimisation et Sécurité des Données (Tech, Produit)** : Mettre en œuvre des mesures techniques de sécurité renforcées, incluant :
    - **Chiffrement renforcé** des données au repos et en transit.
    - **Pseudonymisation** systématique des identifiants et des mesures.
    - **Cloisonnement technique** des bases de données sensibles pour limiter les accès.
    - **Limitation stricte** de la durée de conservation.
5. **Gouvernance de l'IA (Tech, Produit)** : Pour garantir la conformité avec l'AI Act, il est impératif de mettre en place une **architecture en "voting"** avec des sous-modèles fonctionnant en parallèle. Cette approche permettra d'expliquer automatiquement les décisions du système, même si cela implique une potentielle perte d'efficacité.
6. **Audit Externe (Juridique)** : Mandater un **audit externe** pour valider la conformité technique et organisationnelle de la fonctionnalité avant son déploiement, comme spécifié dans le cahier des charges.

La correction de ce traitement critique met en lumière la nécessité d'une gestion rigoureuse du cycle de vie des données, un point abordé dans la section suivante.

Chantier Prioritaire 2 : Inscription « à vie » et Durée de Conservation

Analyse Stratégique : Contexte et Risques

Alors que la vision produit originale incluait des mécanismes conformes comme le renouvellement périodique du consentement, le concept marketing d'inscription "à vie" a conduit à une implémentation en opposition directe avec le principe fondamental de **limitation de la durée de conservation** (Art. 5 RGPD). En conservant les données indéfiniment, le projet nie le droit à l'oubli, augmente les risques en cas de faille de sécurité et crée un risque systémique de surveillance perpétuelle. Ce principe de rétention illimitée amplifie dangereusement les risques associés à chaque autre fonctionnalité non conforme, en particulier le profilage de données sensibles, en créant un répertoire permanent et croissant de données toxiques.

Diagnostic de Non-Conformité

Violations et Risques Identifiés	Criticité / Priorité
Violations RGPD : Art. 5 (limitation de la durée), Art. 17 (droit à l'effacement).	Criticité : Critique Priorité : Immédiate
Risques pour les personnes : Impossibilité d'exercer le droit à l'effacement, traçabilité perpétuelle, perte du droit à l'oubli, surveillance à vie entière.	Criticité : Critique Priorité : Immédiate

Plan d'Action Correctif

1. **Suppression du Concept "à vie" (Produit, Juridique)** : Remplacer immédiatement toute mention d'"inscription à vie" dans les communications et interfaces par une politique de rétention claire. La durée de référence pour les données actives est de **3 ans après la dernière activité du client** (ou dernière commande).
2. **Définition de Politiques de Rétention (Juridique, Tech)** : Définir et documenter des durées de conservation précises et proportionnelles pour chaque finalité de traitement. Ces durées doivent être clairement communiquées aux utilisateurs.
3. **Mise en Œuvre de la Purge Automatique (Tech)** : Développer et déployer des scripts techniques pour assurer la **suppression ou l'anonymisation automatique** des données personnelles une fois que leur durée de conservation définie est expirée.
4. **Garantie du Droit à l'Effacement (Tech, Juridique)** : Mettre en place un processus fonctionnel et accessible pour que les utilisateurs puissent exercer leur droit à

l'effacement (Art. 17). Ce processus doit inclure une **supervision humaine** pour garantir la traçabilité et **l'effacement effectif des données intégrées dans les modèles d'IA (embeddings sensibles)**.

Le profilage, qui exploite également des données sur le long terme, constitue une autre fonctionnalité critique nécessitant une remédiation immédiate.

Chantier Prioritaire 3 : Profilage multidimensionnel sensible

Analyse Stratégique : Contexte et Risques

Le projet de profilage basé sur des données particulièrement sensibles (opinions religieuses, idéologiques, politiques) est, par principe, **interdit** par l'Article 9 du RGPD. Le projet ne dispose actuellement d'aucune dérogation ou base légale valide pour un tel traitement. Cette fonctionnalité n'est pas seulement à risque ; elle est illégale dans son concept même. Les risques de discrimination, de manipulation et de stigmatisation sont maximaux et inacceptables.

Diagnostic de Non-Conformité

Violations et Risques Identifiés	Criticité / Priorité
Violations RGPD : Art. 9 (données sensibles), Art. 6 (absence de base légale), Art. 22 (décision automatisée).	Criticité : Critique Priorité : Immédiate
Risques pour les personnes : Discrimination liée à la religion ou aux opinions, profilage illicite, manipulation, atteinte à la liberté de pensée, biais algorithmique.	Criticité : Critique Priorité : Immédiate

Plan d'Action Correctif

1. **Interdiction par Défaut (Juridique, Produit)** : Le profilage basé sur les catégories de données sensibles est interdit. Il ne pourra être envisagé qu'à la condition stricte d'obtenir un **consentement granulaire, spécifique et explicite** de l'utilisateur pour *chaque* catégorie de donnée sensible concernée.
2. **Mise en Place de la Supervision Humaine (Produit, Tech)** : Implémenter un **contrôle humain obligatoire** pour toute décision significative ou à impact important issue du profilage. Une décision entièrement automatisée basée sur ces données est illégale (Art. 22).
3. **Transparence et Explicabilité (Produit, Tech)** : Fournir à l'utilisateur une **explication claire** sur la logique du profilage, les catégories de données utilisées et les conséquences. Mettre en place un processus simple et accessible pour permettre à l'utilisateur d'exercer son droit d'opposition.
4. **Réalisation d'une AIPD (Juridique)** : La conduite d'une **AIPD** est obligatoire avant toute mise en œuvre de ce traitement pour évaluer formellement les risques et définir les mesures de mitigation adéquates.

5. **Audit des Biais (Tech)** : Réaliser un **audit des biais** pour détecter et corriger tout traitement inéquitable ou discriminatoire généré par les algorithmes de profilage.

Ce profilage individuel se double d'un risque accru lorsqu'il s'étend au cercle familial, posant des défis de conformité supplémentaires.

Plan d'Action pour les Autres Fonctionnalités Non Conformes

Les fonctionnalités suivantes présentent également des non-conformités critiques qui requièrent des actions correctives immédiates.

Suivi familial

- **Problématique Principale** : Le traitement des données de tiers, en particulier de **mineurs**, sans leur consentement ou celui de leurs représentants légaux, et l'absence de base légale pour le profilage du foyer.
- **Actions Correctives Clés** :
    - Mettre en place un mécanisme pour **obtenir le consentement parental explicite** pour tout traitement de données concernant des mineurs. (Juridique, Produit)
    - Implémenter le **masquage de catégories sensibles par défaut** pour les mineurs. (Tech, Produit)
    - **Interdire formellement le profilage par IA sur les données des mineurs** sans le consentement parental explicite. (Juridique, Tech)
    - Configurer la **suppression automatique des données des mineurs** à leur majorité, sauf s'ils consentent personnellement à poursuivre le service. (Tech)

Monitoring communautaire

- **Problématique Principale** : Le profilage à grande échelle des relations sociales et la déduction potentielle d'opinions politiques ou religieuses à partir des graphes relationnels, sans base légale adéquate.
- **Actions Correctives Clés** :
    - **Supprimer le scoring d'influence** et limiter les finalités du traitement à des objectifs légitimes et clairement définis. (Produit)
    - Mettre en place une **anonymisation stricte (de type k-anonymat, avec un k≥10 comme suggéré dans les sources pour les agrégations)** pour toutes les analyses communautaires. (Tech)
    - **Interdire le profilage politique ou religieux** dérivé de l'analyse des réseaux, sauf obtention d'une base légale explicite. (Juridique)
    - Instaurer un **contrôle humain obligatoire** sur toute analyse de réseau social jugée sensible. (Produit)

Envoi automatique de produits de test

- **Problématique Principale** : L'envoi de produits non sollicités s'apparente à une sollicitation commerciale agressive, effectuée sans le consentement préalable, libre et éclairé de l'utilisateur.
- **Actions Correctives Clés** :
    - Remplacer le système actuel par un **consentement préalable obligatoire (opt-in strict)** avant tout envoi de produit. (Produit, Juridique)

    - Intégrer une **validation humaine** dans le processus de sélection et de décision d'envoi. (Produit)
    - Développer un **processus de désinscription simple, immédiat et accessible** ("à un clic"). (Tech)

Recommandation adaptive cross-profil

- **Problématique Principale** : L'inférence d'événements de vie extrêmement privés (divorce, déménagement, changement de carrière) pour adapter les recommandations constitue une décision automatisée intrusive, violant l'Article 22 du RGPD.
- **Actions Correctives Clés** :
    - Assurer une **transparence totale** envers l'utilisateur sur les données utilisées et la logique des algorithmes d'adaptation. (Produit, Tech)
    - Garantir une **intervention humaine obligatoire** dans le processus de décision et offrir un droit de contestation simple et effectif. (Produit)
    - Réaliser un **audit des biais** pour s'assurer que les adaptations ne sont pas discriminatoires ou ne créent pas d'effets de "bulle de filtre" préjudiciables. (Tech, Juridique)

Partage en réseau des recommandations

- **Problématique Principale** : Le concept de "partage forcé" a été rejeté comme étant illégal durant la phase de spécification. Il constitue une violation de la vie privée des tiers destinataires (spam) et une collecte de leurs données sans aucune base légale. Le seul chemin acceptable est un modèle basé sur le consentement.
- **Actions Correctives Clés** :
    - Abandonner le système actuel et le remplacer par un mécanisme de **double opt-in**, où le destinataire doit explicitement accepter de recevoir des recommandations avant toute communication. (Produit, Tech)
    - **Interdire formellement le partage forcé** et toute collecte de données de tiers sans leur consentement préalable. (Juridique)

Chantiers Transverses de Gouvernance

La correction des non-conformités fonctionnelles est insuffisante sans la mise en place d'un cadre de gouvernance robuste. Ce cadre est essentiel pour assurer une conformité durable et systémique.

Cadre Général de Gouvernance des Données

- **Actions à Mettre en Œuvre** :
    - **Registre des Traitements** : Finaliser, documenter et maintenir à jour un registre exhaustif de tous les traitements de données personnelles, en précisant pour chacun la finalité, la base légale, les catégories de données et la durée de conservation. (Juridique)
    - **Politique de Rétention** : Définir, formaliser et appliquer une politique de rétention globale, incluant la mise en œuvre technique de la purge automatique des données. (Juridique, Tech)
    - **Centre de Confidentialité** : Développer une interface utilisateur centralisée et intuitive permettant aux utilisateurs de gérer leurs consentements de manière granulaire et d'exercer facilement leurs droits (accès, rectification, effacement, portabilité). (Produit, Tech)

Cadre de Gouvernance de l'IA

- **Actions à Mettre en Œuvre** :
    - **Politique "Human-in-the-loop"** : Cartographier toutes les décisions algorithmiques, évaluer leur niveau de criticité et imposer une supervision humaine systématique pour toutes les décisions ayant un impact significatif sur les individus. (Produit, Juridique)
    - **Explicabilité (XAI)** : Documenter tous les modèles d'IA via des **"model cards"** détaillées et implémenter des outils techniques permettant d'expliquer les décisions individuelles, tant pour les utilisateurs que pour les auditeurs internes et externes. (Tech)
    - **Audits Réguliers** : Planifier et exécuter des audits périodiques des systèmes d'IA pour détecter les biais, la dérive des modèles ("model drift") et les nouvelles vulnérabilités de sécurité. (Tech, Juridique)

Prochaines Étapes et Pilotage du Plan d'Action

Synthèse Finale

L'urgence et la criticité des actions listées dans ce plan ne peuvent être sous-estimées. La mise en conformité du projet avec le RGPD et l'AI Act n'est pas une option, mais une condition *sine qua non* à sa poursuite. L'arrêt immédiat des traitements les plus illégaux et le lancement des chantiers prioritaires sont impératifs pour protéger l'entreprise des risques juridiques et préserver la confiance des utilisateurs.

Feuille de Route et Responsabilités

Les prochaines étapes pour le déploiement de ce plan d'action sont les suivantes :

- **Nomination d'un Comité de Pilotage Conformité** réunissant des représentants des équipes Juridique, Produit et Tech pour superviser la mise en œuvre du plan.
- **Attribution d'un "Owner"** pour chaque chantier prioritaire identifié, qui sera responsable de son avancement et du reporting associé.
- **Établissement d'un calendrier prévisionnel** avec des jalons clés pour la mise en œuvre de chaque mesure corrective, en commençant par les actions à priorité "Immédiate".
- **Mise en place d'un reporting régulier** à la direction sur l'état d'avancement du plan de conformité, les points de blocage et les ressources nécessaires.