Cahier des Charges Révisé
Mise en Conformité
RGPD & EU AI Act

Introduction : De la Vision Initiale à une Conception Conforme et Éthique

Ce cahier des charges annule et remplace toute version antérieure. Il mandate un alignement intégral du projet avec les exigences impératives du Règlement Général sur la Protection des Données (RGPD) et les principes de l'EU AI Act. La conception initiale présentait des non-conformités critiques qui exposaient le service et ses utilisateurs à des risques majeurs. Cette version révisée intègre les principes de **Privacy by Design** (protection de la vie privée dès la conception) et d'**Ethical AI by Design** (IA éthique dès la conception) comme des piliers non négociables. Chaque fonctionnalité est repensée pour garantir la protection des droits fondamentaux des utilisateurs, assurer une transparence totale et construire une relation de confiance durable.

Principes Fondamentaux de Conformité

Cadre de Consentement & Minimisation des Données

Le consentement de l'utilisateur et la minimisation des données collectées constituent les fondations de toute interaction au sein de ce projet. La confiance de l'utilisateur repose sur une transparence absolue quant à l'usage de ses informations et sur la possibilité d'exercer un contrôle granulaire et permanent. Toute collecte ou traitement doit être justifié, proportionné et clairement expliqué.

Les règles de gouvernance suivantes s'appliquent de manière transversale à l'ensemble des fonctionnalités :

- **Bases Légales Explicites :** Chaque traitement de données doit impérativement reposer sur une base légale valide (conformément à l'art. 6 du RGPD), qui sera clairement identifiée et documentée dans le registre des traitements. Le consentement explicite (art. 9.2.a RGPD) sera la base légale privilégiée pour toute collecte ou traitement de données sensibles, notamment les données de santé ou biométriques.
- **Consentement Granulaire :** Un centre de confidentialité accessible et simple d'utilisation sera mis en place. Il permettra à l'utilisateur d'activer ou de désactiver chaque finalité de traitement de manière indépendante, garantissant ainsi un choix libre, spécifique et éclairé.
- **Minimisation par Défaut :** Le principe de minimisation est appliqué par défaut. Seules les données strictement nécessaires à la finalité poursuivie et consentie seront collectées et traitées. Toute collecte de données *au cas où* est proscrite.
- **Politiques de Rétention Strictes :** Conformément à l'action corrective identifiée pour le traitement FASH-001, toute conservation illimitée est interdite. Une politique de purge et d'anonymisation automatisée sera implémentée pour supprimer les données personnelles à l'échéance de leur durée de conservation définie et communiquée à l'utilisateur.
- **Séparation des bases de données de production et d'entraînement:** Ce cloisonnement strict est du ressort de l'équipe data, car lié à l'entraînement du modèle IA qui recommande des vêtements; ceci est mis en place afin d'éviter le risque de détournement de finalité de l'IA (Art. 5.1.b RGPD)

Ces principes de collecte et de conservation doivent être complétés par des garanties d'équité dans les décisions prises sur la base de ces données.

Critères d'Éligibilité Transparents et Équitables

Les décisions automatisées, en particulier celles concernant l'éligibilité à un service, présentent des risques élevés de discrimination et d'exclusion. Cette section établit les garde-fous nécessaires pour garantir un accès juste, équitable et non discriminatoire au service, en plaçant la supervision humaine au cœur du processus décisionnel.

Les obligations suivantes sont impératives et non-négociables :

1. **Publication des Règles :** Les règles d'éligibilité (par exemple, la majorité légale ou les pays de résidence supportés) doivent être publiques, claires, objectives et facilement accessibles. Elles ne doivent jamais être fondées sur des critères sensibles ou inférés, tels que l'apparence physique ou un état de santé supposé.
2. **Interdiction de la Décision Automatisée Exclusive :** Toute décision de refus d'éligibilité qui serait assistée par une intelligence artificielle doit obligatoirement être revue et validée par un opérateur humain. Un système entièrement automatisé ne peut pas, à lui seul, exclure un utilisateur.
3. **Droit de Recours Humain :** Un processus de recours simple et efficace doit être mis à la disposition des utilisateurs. En cas de refus, l'utilisateur doit recevoir une notification claire exposant les motifs de la décision et un mécanisme lui permettant de demander un réexamen de son dossier par un humain.

Cette garantie d'équité dans les décisions d'accès se prolonge par une exigence plus large de supervision humaine sur l'ensemble des systèmes algorithmiques.

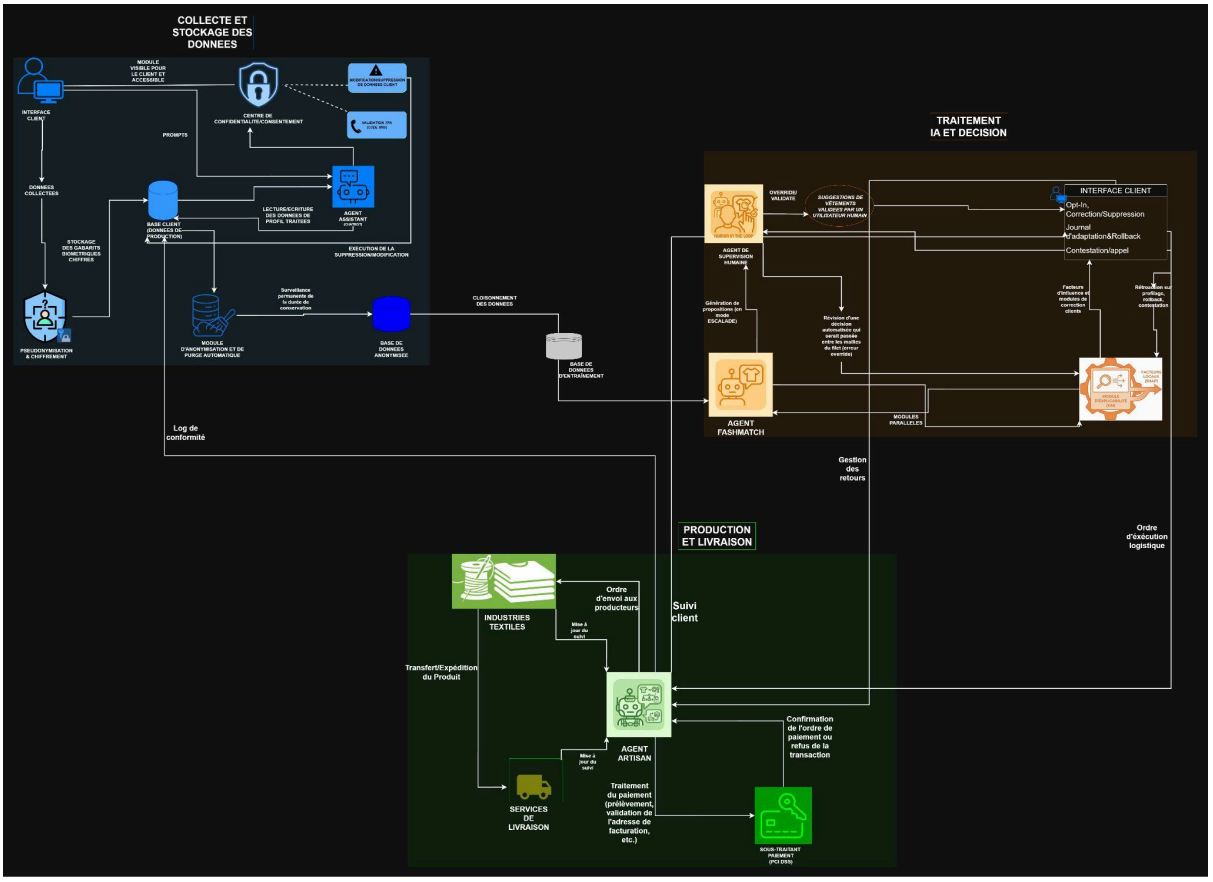
Politique de Supervision Humaine ("Human-in-the-Loop") et d'IA Explicable (XAI)

Une supervision humaine robuste et l'explicabilité des modèles d'IA (XAI) sont cruciales pour maîtriser les risques, garantir la conformité (notamment avec l'article 22 du RGPD sur les décisions automatisées) et maintenir la confiance des utilisateurs. Un algorithme ne peut opérer comme une "boîte noire" lorsque ses décisions ont un impact significatif sur les individus.

Les directives suivantes sont donc mandatées :

- **Cartographie des Risques :** Une classification de toutes les décisions algorithmiques selon leur niveau de risque (faible, modéré, élevé, critique) doit être réalisée. Une revue humaine systématique est obligatoire pour toutes les décisions identifiées comme ayant un impact significatif sur les personnes.
- **Explicabilité par Conception :** L'utilisation de techniques d'IA explicable (XAI) est mandatée. Pour chaque recommandation ou décision importante, le système doit être capable de fournir à l'utilisateur les principaux facteurs qui ont influencé ce résultat, dans un langage clair et compréhensible.
- **Mécanismes de Contrôle Humain :** Des processus clairs d'escalade vers un support humain doivent être implémentés. Les opérateurs doivent disposer de droits de veto (*override*) pour corriger les décisions erronées des algorithmes, et des mécanismes d'arrêt d'urgence (*kill-switch*) doivent être prévus pour désactiver tout système d'IA présentant un comportement imprévu ou préjudiciable.

Les fonctionnalités initialement envisagées sont désormais révisées à la lumière de ces principes fondamentaux, ce qui nous permet de proposer l’architecture suivante:



En version plus claire ici: archi_fashmatch(svg).drawio.svg

Considérant les flux représentés sur le graphe, de la collecte des données client à la gestion des retours, les phases suivantes détaillent l'architecture FashMatch:

Phase 1: Collecte, Consentement et Cycle de Vie des Données (Zone Bleue - Collecte et Stockage des données)

Tout commence par l'interaction du Client avec l'Interface Client, qui est le point d'entrée pour la collecte et la gouvernance des données.

1. **Collecte sous consentement granulaire:** La relation initiale est encadrée par le **Cadre de Consentement & Minimisation des Données. L**e Client doit fournir un **consentement explicite, spécifique et éclairé (Art. 9.2.a RGPD)** pour l'activation de chaque finalité de traitement (profilage, analyse biométrique, etc.). Ce choix est géré dans le **Centre de Confidentialité.**

2. **Flux Biométrique Sécurisé:** Les données sensibles (photos, vidéos, données de santé) ne sont pas stockées brutes. Elles transitent par un **Module de Pseudonymisation & Chiffrement renforcé** avant d'être écrites dans la **Base client des données d'entraînement.** Seuls les **gabarits biométriques chiffrés** (et non les photos originales) sont conservés. Le Cahier des charges révisé exige une

Analyse d'Impact (AIPD) complète pour ce flux avant tout développement.

3. **Rétention et Purge Automatique:** Le concept illégal d'Inscription à vie est abandonné. **La Base de données n'est plus statique**. Le **Module de Purge Automatique** (nouveau composant essentiel) surveille en permanence la durée de conservation. Après une durée définie (par exemple, 36 mois d'inactivité), le module déclenche la suppression ou l'anonymisation des données personnelles non essentielles.

4. **Exercice des Droits:** Le Client peut déclencher le flux de **Modification ou suppression** de données client (via l'Interface Client). Ce flux permet l'export complet (portabilité) et la suppression complète du compte. Ce processus de suppression doit inclure une **Supervision humaine** pour garantir l'effacement effectif des **embeddings sensibles intégrés dans les modèles d'IA**.

Phase 2: Traitement IA, Supervision et Explicabilité (Zone Orange - Traitement IA et Décision)

La **Base de données anonymisée alimente l'AGENT FASHMATCH** pour la personnalisation. Cependant, plusieurs exclusions s'appliquent : les **données sensibles illicites (religieuses, politiques) sont techniquement bloquées** et ne doivent pas atteindre l'AGENT FASHMATCH, et la fonctionnalité de Scoring psycho-comportemental est supprimée du système car jugée Inacceptable (Pratique Interdite Art. 5 AI Act).

1. **Génération de propositions: L'AGENT FASHMATCH** (l'intelligence artificielle centrale) génère des Propositions (recommandations, adaptations de profil, sélection de produits) en s'appuyant sur les données de profilage non sensibles.

2. **Flux d'Escalade HIL (Intervention Humaine Obligatoire):** La loi interdit que l'IA prenne seule une décision à impact significatif. Pour les décisions critiques (refus d'éligibilité, adaptations intrusives, proposition d'envoi), l'AGENT FASHMATCH ne peut pas agir directement. Il déclenche un **flux d'Escalade vers l'Opérateur HIL (Agent de Supervision Humaine)**.

3. **Flux d'Override HIL: L'opérateur HIL audite le cas remonté.** Il dispose du droit d'Override (veto) pour annuler une décision jugée biaisée, discriminatoire ou erronée. Une fois la décision validée ou corrigée par l'humain, elle peut être transmise aux systèmes d'exécution.

4. **Flux de Contestation (Client vers HIL):** Le Client peut initier le processus HIL en sens inverse. Si le Client conteste une adaptation de profil ou un refus d'éligibilité, l'Interface Client déclenche un canal dédié qui route le cas vers l'Opérateur HIL pour

un réexamen humain, garantissant ainsi le droit de recours.

5. **Flux d'Explicabilité (XAI):** Le **Module d'Explicabilité (XAI)** fonctionne en parallèle de l'AGENT FASHMATCH. Ce module génère les **facteurs locaux expliquant une décision ou une adaptation**. Ce flux de **Transmission d'Explication** alimente directement l'Interface Client dans des sections comme **"Ce qui a changé dans votre profil"**, répondant ainsi aux obligations de transparence (Art. 13 & 14).

6. **Flux de Rétroaction Client:** Le Client peut interagir avec les explications via l'Interface Client. Il peut déclencher un **Rollback** pour annuler les adaptations de profil récentes ou un **flux de Correction/Suppression d'Inférence** pour mettre à jour la logique du profilage non sensible.

Phase 3: Exécution de Commande et Logistique (Zone Verte - Production et Livraison)

Le flux logistique est activé uniquement par l'ordre de commande issue du client (via l'interface client);

1. **Rupture du Flux Automatisé: L'AGENT FASHMATCH (sélecteur par IA) ne peut JAMAIS se lier directement à l'AGENT ARTISAN (Logistique**). Cette rupture est essentielle pour éviter le risque d'envoi non consenti.

2. **Déclenchement par le Client (Confirmation Finale):**

    - La proposition de produit (validée ou non par l'Opérateur HIL) est d'abord envoyée à l'**Interface Client**.
    - Le Client doit donner une **Confirmation Finale** (opt-in pour l'envoi spécifique, ex: "Confirmez-vous l'envoi de ce produit ?").
3. **Ordre de Production et Paiement: Seule la Confirmation Finale du Client génère l'Ordre de Production** (jeton d'autorisation) qui est transmis à l'**AGENT ARTISAN** (Orchestration logistique).

    - L'AGENT ARTISAN initie ensuite le flux de paiement auprès du **Sous-Traitant Paiement (PCI DSS)** pour valider la transaction, conformément aux normes de sécurité.
4. **Orchestration Logistique:** Une fois la transaction validée, l'**AGENT ARTISAN** transmet l'ordre de production et les spécifications d'emballage aux **Industries qui produisent les vêtements(Fournisseurs)**.

5. **Expédition et Suivi:** Les **Industries qui produisent** préparent et confient le colis au **Service de Livraison (transporteur)**. L'information de suivi est renvoyée par ces acteurs à l'**AGENT ARTISAN**.

6. **Mise à jour Client et Conformité:** L'**AGENT ARTISAN** transmet le statut de la livraison à l'**Interface Client**. Crucial pour la conformité, l'**AGENT ARTISAN**

journalise l'exécution de l'ordre, le lien avec le consentement spécifique du client, et la preuve de livraison dans le **Registre des Consentements (Base Client).**

7. **Gestion des Retours:** Le **Client** initie la demande de retour via l'**Interface Client** (portail retour simple). L'**AGENT ARTISAN** orchestre la logistique inverse (enlèvement, remboursement/avoir) et met à jour les statuts de stock et les systèmes de paiement.

Spécifications Fonctionnelles Révisées

Analyse Biométrique & Physiologique (Version Conforme)

La fonctionnalité d'analyse biométrique est strictement recadrée. En raison du traitement de données de santé, qui constituent une catégorie particulière de données au sens de l'article 9 du RGPD, ce module est désormais conçu comme un outil de suivi personnel, *non médical*, et entièrement *optionnel*. Son activation ne pourra se faire que sur la base d'un consentement explicite, spécifique et éclairé de l'utilisateur pour chaque type d'analyse.

Hypothèses

- Une Analyse d'Impact sur la Protection des Données (AIPD) complète sera réalisée et validée par le DPO avant le démarrage de tout développement.
- Le stockage des données doit se faire sous forme de gabarits biométriques chiffrés (pas de photos brutes)
- Ce module n'est pas un dispositif médical et ne fournit aucun diagnostic.

Fonctionnalités

1. **Capture & Cadence :** Permettre à l'utilisateur de soumettre des photos mensuelles et des vidéos d'activité, avec des rappels configurables.
2. **Historique de Santé (Non-Médical) :** Permettre la saisie et l'édition d'informations contextuelles fournies par l'utilisateur (ex: poids, taille, mobilité générale, événements non médicaux pertinents).
3. **Extraction Morphométrique (Non-Diagnostique) :** Extraire des repères corporels relatifs (posture, mobilité) à partir des médias fournis par l'utilisateur, à des fins de suivi personnel uniquement.
4. **Tendances & Détections Personnelles :** Afficher des séries temporelles et des variations significatives basées sur les données fournies pour aider l'utilisateur à visualiser son évolution personnelle.
5. **Dashboard & Rapports :** Fournir des visualisations claires, des résumés et des comparatifs personnels dans un tableau de bord sécurisé.
6. **Gouvernance & Consentements Granulaires :** Mettre en place un centre de contrôle où l'utilisateur donne un consentement distinct pour la capture de photos, un autre pour la capture de vidéos, et un consentement spécifique pour chaque type d'analyse. L'export et la suppression des données sont accessibles en un clic.
7. **Audit de Biais et de Sécurité par un Tiers :** Imposer une revue périodique des algorithmes et des mesures de sécurité par un tiers de confiance indépendant afin de détecter et mitiger les biais et les vulnérabilités.

User Stories

- **6.a :** "En tant qu'Utilisateur, je veux donner ou retirer mon consentement *spécifiquement* pour l'analyse de mes photos, indépendamment de l'analyse de mes vidéos, afin de maîtriser précisément l'usage de mes données les plus sensibles."

La gestion du cycle de vie de ces données sensibles est tout aussi critique que les conditions de leur collecte.

Gestion du Compte et Rétention des Données (Remplace "Inscription à vie")

Le concept d'"inscription à vie" est en contradiction directe avec le principe de limitation de la durée de conservation imposé par le RGPD. Cette section est donc entièrement réécrite pour définir un cadre de gestion de compte durable, mais respectueux du droit à l'effacement et des durées de rétention proportionnées à la finalité du service.

Contexte et Objectifs

Offrir une continuité de service et un suivi personnalisé sur le long terme, dans le respect de politiques de rétention de données strictes et transparentes communiquées à l'utilisateur.

Fonctionnalités

1. **Cycle de Vie du Compte :** Définir et gérer les différents états du compte : *actif*, *inactif* (période précédant la purge automatique), et *supprimé*.
2. **Dimensions Personnelles Activables :** Permettre à l'utilisateur d'activer ou désactiver des dimensions de suivi (bien-être non médical, préférences, etc.) avec un contrôle *opt-in/opt-out* granulaire.
3. **Politique de Rétention Automatisée :** Mettre en œuvre une fonctionnalité système qui anonymise ou supprime automatiquement les données personnelles à l'expiration des durées de conservation définies. La règle est : **Base active 3 ans après dernière commande, archive intermédiaire 5 ans**. **purge automatique ou anonymisation après 36 mois d'inactivité** (Art. 17, droit à l'effacement; Art. 13-14, information)
4. **Portabilité et Suppression :** Garantir un droit à l'export complet des données et un droit à l'effacement simple et effectif, incluant une supervision humaine pour les cas de suppression complexes (ex: données intégrées dans les modèles d'IA); Le processus de suppression doit garantir l'**effacement effectif des embeddings sensibles** des modèles d'IA
5. **Orchestration des Consentements :** Gérer le cycle de vie des consentements, incluant leur renouvellement périodique, les rappels, et la dégradation maîtrisée des services en cas d'expiration.
6. **Legs Numérique Contrôlé :** Permettre à l'utilisateur de définir des préférences pour la gestion de son compte en cas de décès (ex: mémorialisation, purge complète, transfert restreint), activables sur la base d'un processus vérifié et dans le respect des contraintes légales et des durées de rétention.

User Stories

- **3.a :** "En tant qu'Utilisateur, je veux connaître les durées de conservation de mes données lors de mon inscription, afin de prendre une décision éclairée."
- **4.a :** "En tant qu'Utilisateur, je veux déclencher la suppression complète et irréversible de mon compte et de toutes mes données associées, afin d'exercer mon droit à l'oubli."
- **6.a :** "En tant qu'Utilisateur, je veux définir des directives claires sur le sort de mes données après mon décès (purge ou mémorialisation), afin de gérer mon héritage numérique de manière conforme."

Au-delà de la durée de vie du compte, la nature des données de profilage doit également être strictement encadrée.

Profilage Contrôlé et Non-Sensible (Remplace "Profilage multidimensionnel")

Le profilage basé sur des données sensibles telles que les opinions religieuses ou politiques est interdit par l'article 9 du RGPD, sauf à disposer d'une base légale exceptionnelle. Cette section réoriente la fonctionnalité vers un profilage basé exclusivement sur les préférences déclarées par l'utilisateur et les comportements observés sur la plateforme, le tout sous son contrôle strict et permanent.

Contexte et Objectifs

Construire un profil de préférences sous le contrôle de l'utilisateur, en distinguant clairement les données qu'il a déclarées de celles inférées par le système, et en offrant des mécanismes simples de correction et de suppression. L'extraction de catégories spéciales de données est formellement interdite.

Fonctionnalités

1. **Connexions aux Sources de Données (Optionnel) :** Permettre la connexion à des sources externes (ex: réseaux sociaux) via des mécanismes OAuth, avec des scopes d'autorisation minimaux et une prévisualisation claire des données collectées.
2. **Gestion des Centres d'Intérêt :** Fournir une interface où l'utilisateur sélectionne, ajoute ou supprime manuellement ses centres d'intérêt à partir d'une liste prédéfinie et garantie non-sensible.
3. **Transparence & Correction du Profil :** Mettre à disposition un tableau de bord où l'utilisateur peut visualiser toutes les données composant son profil, connaître l'origine de chaque information (*déclarée* vs. *inférée*), et la corriger ou la supprimer en un clic.
4. **Audit des Biais Algorithmiques :** Intégrer une fonctionnalité système pour tester et mitiger régulièrement les biais discriminatoires (liés au genre, à l'âge, etc.) dans les algorithmes de profilage.

5. **Interdiction formelle d’utiliser ou d’inférer les données sensibles (religieuses, idéologiques, politiques) par l’IA:** Insérer une note d’interdiction formelle dans la section *Fonctionnalités ou Contexte,* afin de bloquer techniquement cette catégorie de données illégale (Art. 9, données sensibles; Art. 6, base légale).
6. **Gouvernance et Droits :** Maintenir un journal des consentements, garantir un droit d'opposition effectif à tout profilage et interdire par conception tout usage discriminatoire des données de profil. Toute décision significative issue du profilage requiert une intervention humaine.

User Stories

- **2.a :** "En tant qu'Utilisateur, je veux sélectionner manuellement mes centres d'intérêt à partir d'une liste, afin de contrôler les bases de ma personnalisation."
- **3.a :** "En tant qu'Utilisateur, je veux visualiser une inférence faite par le système (ex: 'aime le style X') et la supprimer, afin que mon profil reflète fidèlement mes goûts."

La problématique du consentement et du contrôle de l'individu doit également s'appliquer rigoureusement au cercle familial.

Suivi des Dépenses du Foyer (Remplace "Suivi familial")

Le suivi des achats d'un foyer, en particulier lorsqu'il inclut des mineurs, présente des risques élevés pour la vie privée de chaque membre. La fonctionnalité est entièrement repensée pour exiger le consentement individuel et révocable de chaque membre adulte, ainsi que le **consentement parental pour les mineurs de moins de 15 ans**, avec des mesures de protection renforcées pour ces derniers.

Hypothèses

- Le profilage par IA sur les données des mineurs est strictement interdit sans le consentement explicite et spécifique des titulaires de l'autorité parentale (Art. 6, base légale; Art. 8, consentement mineurs).

Fonctionnalités

1. **Modèle de Foyer et Membres Consentis :** Mettre en place un flux de *double opt-in* où chaque membre adulte doit donner son consentement explicite pour rejoindre le foyer et partager ses données de transaction.
2. **Protection Renforcée des Mineurs :** Masquer par défaut toutes les données relatives aux mineurs et interdire leur utilisation à des fins de profilage ou de recommandation. Toute visibilité ou traitement requiert une action positive des titulaires de l'autorité parentale.
3. **Filtrage Technique :** Exclure les données des mineurs des datasets de profilage marketing, même si le consentement parental est obtenu; ceci permet de remédier au **Profilage d'enfants, jugé Critique.**
4. **Connexion aux Comptes & Agrégation :** Permettre l'import sécurisé des transactions via des agrégateurs conformes (*read-only*) et leur catégorisation.
5. **Moteur d'Attribution Assisté :** Proposer une attribution probable des achats aux membres du foyer, avec un score de confiance et une explication, tout en permettant une correction manuelle facile.
6. **Gouvernance & Confidentialité Granulaire :** Permettre à chaque membre adulte de contrôler les catégories d'achats (ex: santé, loisirs) qu'il accepte de partager avec les autres membres du foyer.

User Stories

- **2.a :** "En tant que Parent, je veux que les données de mon enfant soient masquées par défaut et ne soient jamais utilisées pour la recommandation de produits, afin de protéger sa vie privée."
- **5.a :** "En tant que Conjoint, je veux exclure certaines catégories de dépenses (ex: santé) du suivi familial, afin de préserver mon jardin secret."

Cette granularité de contrôle doit s'étendre de la sphère privée du foyer à la sphère sociale de la communauté.

Analyse des Tendances Communautaires (Remplace "Monitoring communautaire")

Le concept de "monitoring" individuel est abandonné au profit d'une analyse de tendances agrégées et anonymisées. L'objectif n'est plus de surveiller ou de noter l'influence des individus, mais de dégager des courants de fond au sein de la communauté, dans le respect strict de la vie privée et avec une interdiction formelle de tout profilage politique ou idéologique.

Hypothèses

- Le principe de **k-anonymisation** est appliqué : aucune agrégation ou tendance ne sera calculée ou affichée si elle est basée sur un groupe de moins de 'k' membres (k=10), afin d'empêcher toute ré-identification.

Fonctionnalités

1. **Ingestion de Signaux Communautaires Consentis :** Collecter des signaux (parrainages, interactions in-app, etc.) uniquement sur la base d'un *opt-in* explicite de l'utilisateur.
2. **Analyse de Tendances Agrégées :** Se concentrer sur les produits, services et catégories populaires au sein de larges groupes d'utilisateurs, sans jamais révéler d'informations individuelles. Le scoring d'influence personnel est supprimé.
3. **Groupes & Challenges (Opt-in) :** Permettre aux utilisateurs de créer ou rejoindre des groupes d'intérêt sur la base du volontariat.
4. **Filtres Éthiques :** Intégrer une fonctionnalité système qui interdit activement l'utilisation du graphe relationnel pour inférer des opinions politiques, religieuses, ou toute autre affiliation sensible.
5. **Gouvernance & Consentements :** Permettre à l'utilisateur de se retirer complètement des analyses de tendances communautaires. Cette option est *désactivée par défaut*.

User Stories

- **2.a :** "En tant qu'Utilisateur, je veux voir les produits qui sont populaires dans ma communauté *sans que le nom des acheteurs ne soit révélé*, afin de découvrir des tendances tout en respectant la vie privée de chacun."
- **5.a :** "En tant qu'Utilisateur, je veux pouvoir me retirer complètement des analyses de tendances communautaires, afin que mes données ne soient jamais utilisées à cette fin."

Les actions proactives basées sur ces données, comme l'envoi de produits, doivent être encore plus rigoureusement encadrées.

Programme de Découverte de Produits sur Invitation (Remplace "Envoi automatique de produits de test")

L'envoi non sollicité de produits s'apparente à du "spam physique" et constitue une pratique commerciale intrusive et non conforme. Cette fonctionnalité est complètement transformée en un programme sur la base du volontariat (*opt-in*), où l'utilisateur consent explicitement à recevoir des propositions de produits, avec un contrôle total sur la fréquence, les catégories d'intérêt et les plafonds budgétaires.

Contexte et Objectifs

Proposer aux utilisateurs volontaires de découvrir des produits, dans un cadre transparent, consenti et maîtrisable.

Fonctionnalités

1. **Éligibilité & Préférences (Opt-in) :** L'utilisateur doit activer le programme et définir ses préférences : catégories de produits autorisées, quotas d'envoi mensuels, et plafonds budgétaires.
2. **Moteur de Sélection avec Validation Humaine :** Le système d'IA peut *proposer* une sélection de produits pertinents. Cependant, chaque proposition générée par l'IA doit être soumise à une file de validation humaine avant d'être présentée à l'utilisateur pour confirmation finale.
3. **Confirmation Finale de l'Utilisateur :** Aucun produit n'est expédié sans que l'utilisateur n'ait donné son accord final sur une proposition spécifique (ex: via une notification "Confirmez-vous l'envoi de ce produit ?").
4. **Logistique & Retours Simplifiés :** Gérer l'expédition, le suivi, et un processus de retour simple et sans friction pour les produits non désirés.
5. **Gouvernance et Registre des Consentements :** Maintenir un registre auditable de tous les consentements (adhésion au programme et validation de chaque envoi) et intégrer des contrôles stricts anti-abus.

User Stories

- **1.a :** "En tant qu'Utilisateur, je veux activer le programme en définissant un budget mensuel maximal de 50€ et en n'acceptant que la catégorie 'soins du corps', afin de contrôler totalement les envois."
- **3.a :** "En tant qu'Utilisateur, je veux recevoir une notification 'Nous pensons que ce produit pourrait vous plaire. Confirmez-vous son envoi ?', afin de donner mon accord final avant chaque expédition."

Cette personnalisation maîtrisée des produits doit trouver son équivalent dans la personnalisation des recommandations algorithmiques.

Recommandation Adaptive et Transparente (Remplace "Recommandation adaptive cross-profil")

Adapter les recommandations aux événements de la vie d'un utilisateur est une fonctionnalité puissante, mais qui comporte des risques élevés d'intrusion et de manipulation. La nouvelle approche est fondée sur la transparence radicale, l'explicabilité et le contrôle de l'utilisateur. Celui-ci doit pouvoir comprendre pourquoi ses recommandations changent, contester une adaptation et même l'annuler.

Objectifs Clés

Respecter les obligations de l'article 22 du RGPD en garantissant la transparence, le droit d'opposition et une intervention humaine pour les adaptations significatives.

Fonctionnalités

1. **Détection d'Événements de Vie (Consentie) :** Identifier des changements significatifs (ex: déménagement) à partir de motifs d'achats, uniquement sur la base de signaux consentis.
2. **Transparence & Explications :** Créer une section dédiée "Ce qui a changé dans votre profil" expliquant en langage clair les raisons de l'évolution des recommandations (ex: "Nous avons remarqué des achats dans la région de Lyon, nous vous proposons donc des offres locales.").
3. **Journal d'Adaptations & Rollback :** Fournir un historique des adaptations du profil et un mécanisme pour "revenir à son profil d'il y a une semaine" si l'utilisateur juge les nouvelles recommandations non pertinentes.
4. **Cross-profil Contrôlé :** L'utilisation des signaux du foyer ou de la communauté pour la recommandation individuelle est *désactivée par défaut* et requiert un *opt-in* explicite de l'utilisateur.
5. **Audit Périodique des Biais :** Mettre en place des tests systématiques pour détecter et mitiger les biais discriminatoires dans l'algorithme d'adaptation.

User Stories

- **1.a :** "En tant qu'Utilisateur, suite à une séparation, je veux que le système détecte le changement dans mes achats et me propose une option pour 'réinitialiser mes préférences', afin de ne plus voir de suggestions liées à mon ex-partenaire."
- **2.a :** "En tant qu'Utilisateur, je veux une page qui m'explique que mes recommandations ont changé parce que j'ai récemment acheté des articles de sport, afin de comprendre la logique du système."

Enfin, le principe de consentement doit s'étendre au-delà de l'utilisateur lui-même, en particulier lorsqu'il s'agit de partage.

Partage en Réseau sur Invitation (Remplace "Partage en réseau des recommandations")

Le concept de "partage forcé" est illégal (anti-spam, RGPD). Cette fonctionnalité est entièrement repensée pour devenir un outil de partage volontaire, basé sur un système d'invitation et de *double opt-in* qui protège scrupuleusement la vie privée et le consentement des destinataires.

Hypothèses

- Aucune communication n'est envoyée à un tiers sans son consentement préalable et explicite.

Fonctionnalités

1. **Flux d'Invitation et de Consentement (Double Opt-in) :** L'utilisateur A envoie une *invitation* à B. B reçoit un message clair ("A souhaite partager des recommandations avec vous. Acceptez-vous ?"). Seul un clic de B sur "Accepter" active le partage.
2. **Partage Contrôlé par l'Émetteur :** Permettre à l'utilisateur de définir les audiences, la durée de visibilité et de masquer des items spécifiques lors du partage.
3. **Traçage Conforme et Anonymisé :** Mesurer l'impact du partage uniquement via des statistiques agrégées respectant la **k-anonymisation**. Tout traçage individuel des actions du destinataire est interdit.
4. **Interdiction du Shadow Profiling:** Bloquer toute création de “profil fantôme” pour les contacts non inscrits, afin d’éviter la propagation automatique de données de tiers (Art. 21, opposition).
5. **Gouvernance et Désinscription Facile :** Maintenir un registre auditable des consentements de partage. Chaque communication envoyée doit contenir une option de désinscription simple, immédiate et permanente.

User Stories

- **1.a :** "En tant que Destinataire (ami de l'utilisateur), je veux recevoir un email me demandant si j'accepte de recevoir des recommandations de la part de [Nom de l'Utilisateur], afin de pouvoir refuser si je ne suis pas intéressé."
- **4.a :** "En tant que Destinataire, je veux un lien 'Se désinscrire' en bas de chaque recommandation partagée, afin de cesser immédiatement toutes les communications futures."