

# Cahier des Charges Final – Projet FashMatch V2

## Conformité RGPD, AI Act et Architecture Data/IA

Skander Saadoune/Mohamed Ahmedvall/Thomas Di Landro

## Contents

<b>1 Contexte, Vision et Justification du Pivot du Projet</b>	<b>3</b>
1.1 Vision Initiale de FashMatch . . . . .	3
1.2 Fonctionnement Actuel — Analyse complète de la Version 1 . . . . .	3
1.3 Problématique et Justification du Pivot . . . . .	4
1.4 Objectif du Cahier des Charges — Définition de la V2 . . . . .	5
<b>2 Analyse du Fonctionnement de la Version 1</b>	<b>5</b>
2.1 Architecture fonctionnelle de l'application <b>FashMatch</b> . . . . .	5
2.2 Collecte des données . . . . .	6
2.3 Profilage et décisions . . . . .	7
2.4 Conclusion – Analyse de la V1 . . . . .	7
<b>3 Présentation de la version 2 de l'application FashMatch</b>	<b>8</b>
<b>4 Analyse Réglementaire : RGPD &amp; AI Act</b>	<b>10</b>
4.1 Approche par les risques du Règlement IA (AI Act) . . . . .	10
4.2 Risques RGPD . . . . .	11
4.3 Risques AI Act . . . . .	12
<b>5 Matrice des Risques Fusionnée</b>	<b>12</b>
<b>6 Architecture V2 – Vue d'Ensemble</b>	<b>13</b>
6.1 Agent Client – Taste Encoder (Local) . . . . .	13
6.2 Serveur IA – Moteur de Matching Vectoriel . . . . .	13
6.3 Essayage Virtuel (Virtual Try-On) . . . . .	14
<b>7 Parcours Utilisateur et Enrôlement</b>	<b>14</b>
7.1 Inscription Sécurisée (Vérif-ID) . . . . .	14
7.2 Connexion et Gestion des Consentements . . . . .	14
<b>8 Moteur de Recommandation Hybride</b>	<b>14</b>
8.1 Composant Local – Taste Encoder . . . . .	14
8.2 Composant Serveur – FashMatch . . . . .	14
<b>9 Visualisation – Essayage Virtuel</b>	<b>15</b>
<b>10 Gestion des Artisans</b>	<b>15</b>

<b>11 Architecture Technique</b>	<b>15</b>
11.1 Microservices . . . . .	15
11.2 Sécurité – Zero Trust . . . . .	15
<b>12 Conclusion</b>	<b>16</b>

# 1 Contexte, Vision et Justification du Pivot du Projet

Ce document fusionne l'ensemble des livrables demandés dans le projet “*À la croisée des Arts*” (Projet Commun MSc DPO/Data-IA) et constitue le **cahier des charges final**, conforme aux exigences du sujet [1].

FashMatch est une application de **Fashion Tech** basée sur l'IA permettant des recommandations vestimentaires hyper-personnalisées. Elle met en relation les utilisateurs avec des artisans créateurs et s'appuie, dans sa version initiale, sur un modèle d'intelligence artificielle générative exploitant massivement les données personnelles.

## 1.1 Vision Initiale de FashMatch

FashMatch est conçue comme une application mobile de *Personal Shopper* alimentée par l'IA. Elle ambitionne d'offrir des recommandations vestimentaires sur-mesure en combinant analyse morphologique, goûts personnels, tendances et artisanat créatif.

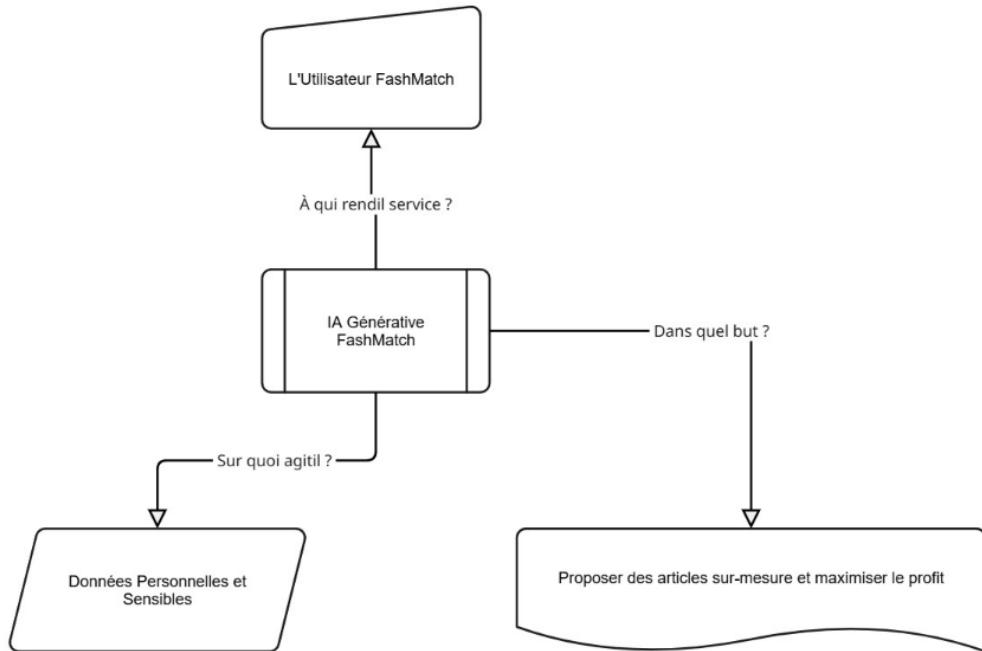


Figure 1: Schéma conceptuel de la V1 : données utilisées, logique interne et objectif commercial.

## 1.2 Fonctionnement Actuel — Analyse complète de la Version 1

La **Version 1 (V1)** repose sur une stratégie de **profilage agressif**, collectant massivement des données sensibles dans le but d'influencer le comportement d'achat. Elle

centralise un très grand volume d'informations, notamment :

- photos et vidéos,
- données sonores,
- informations familiales (enfants, conjoint, réseau proche),
- données issues des réseaux sociaux,
- données sentimentales, relationnelles et comportementales,
- informations de santé (IMC, morphologie, activité, historique médical),
- données financières et de paiement.

L'IA de FashMatch V1 réalise ensuite :

- un **suivi à vie** du client et des tiers associés,
- un **profilage multidimensionnel** (religion, idées, sentiments, habitudes professionnelles),
- un **profilage biométrique** (IMC, morphologie, silhouette),
- un **filtrage automatique des inscriptions** basé sur l'âge estimé,
- l'**envoi automatique de produits non sollicités** pour influencer les achats,
- des **décisions entièrement automatisées et non supervisées**.

Les finalités commerciales de la V1 sont explicites :

- maximisation du ROI par l'influence d'achat,
- exploitation des réseaux sociaux et communautés d'utilisateur,
- modulation comportementale via l'IA générative,
- analyse psychologique et sociale pour augmenter le panier moyen.

### 1.3 Problématique et Justification du Pivot

La V1 présente de nombreux **risques critiques** :

- collecte excessive et non minimisée de données personnelles,
- traitement de données biométriques, psychologiques et sociales,
- absence totale de supervision humaine,
- décisions automatisées excluantes,
- mécanismes de manipulation comportementale,
- envoi automatisé de produits non demandés,

- exploitation de la vulnérabilité des mineurs via l'estimation d'âge.

Ces pratiques placent FashMatch V1 dans la catégorie des :

- **risques inacceptables de l'AI Act** [3],
- violations majeures du **RGPD** (licéité, minimisation, proportionnalité, consentement) [2].

La V1 est donc **juridiquement non viable**. Son maintien expose l'entreprise à des sanctions réglementaires lourdes, un risque réputationnel massif et une impossibilité de mise sur le marché dans l'Union Européenne.

## 1.4 Objectif du Cahier des Charges — Définition de la V2

L'objectif du présent cahier des charges est de formaliser la **Version 2 (V2)** de FashMatch, reposant sur une architecture :

- **Zero Trust**,
- **Federated Learning**,
- **Anonymisation irréversible**,
- **Privacy-by-Design et Privacy-by-Default**,
- **Supervision humaine systématique (HITL)**.

La V2 vise à maintenir un très haut niveau de personnalisation tout en garantissant une conformité totale aux exigences du RGPD et du AI Act.

## 2 Analyse du Fonctionnement de la Version 1

### 2.1 Architecture fonctionnelle de l'application FashMatch

L'application **FashMatch** repose sur une architecture multi-agents interconnectée permettant d'assurer une expérience fluide entre les clients, les artisans et les fournisseurs. Le système est structuré autour de trois agents principaux : l'**Agent Assistant**, l'**Agent FashMatch** et l'**Agent Artisan**.

**Agent Assistant** L'Agent Assistant est responsable de la collecte et de la centralisation de l'ensemble des informations relatives aux clients. Il gère notamment les données personnelles, les informations de paiement (coordonnées, carte bancaire, adresse), ainsi que les préférences stylistiques. Toutes ces données sont ensuite enregistrées dans la **Base Clients** afin de constituer un profil complet et exploitable.

**Agent FashMatch** L'Agent FashMatch constitue le cœur décisionnel du système. Il exploite la **Base Clients** afin d'analyser les préférences et les besoins des utilisateurs. À partir de ces éléments, il génère des **recommandations personnalisées** et les transmet directement au client. Il est également connecté à la **Base Artisans**, afin d'identifier les produits les plus pertinents pour chaque profil.

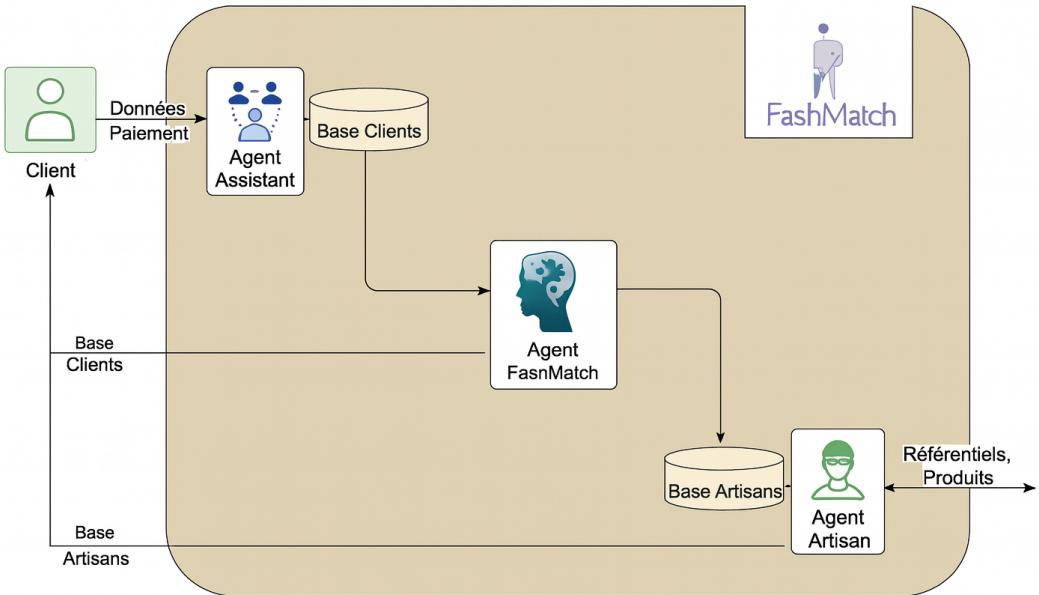


Figure 1 : Architecture fonctionnelle de l'application *FashMatch*.

Figure 2: Architecture fonctionnelle de l'application *FashMatch*.

**Agent Artisan** L'Agent Artisan gère l'interaction avec les artisans et les fournisseurs. Il est connecté au **référentiel produits** pour récupérer les catalogues, nouveautés et stocks disponibles. Ces informations alimentent la **Base Artisans**, utilisée ensuite par l'Agent FashMatch pour la construction des recommandations. Lorsque l'utilisateur commande, l'Agent Artisan orchestre la mise à disposition ou la livraison des produits.

### Synthèse des flux principaux

- **Client → Agent Assistant → Base Clients** : collecte et enregistrement des données.
- **Agent FashMatch → Client** : envoi des recommandations personnalisées.
- **Agent Artisan Fournisseurs** : gestion et mise à jour des référentiels produits.
- **Agent FashMatch Agent Artisan** : sélection et transmission des produits recommandés.

## 2.2 Collecte des données

La version 1 de FashMatch repose sur une collecte **massive** et **multimodale** de données, couvrant :

- des photos (tous formats),
- des vidéos,
- des extraits sonores,

- des données personnelles et familiales,
- des liens vers les réseaux sociaux,
- des contacts relationnels,
- des données de paiement,
- des données comportementales,
- des données de santé (IMC, morphologie, activité).

Ces données alimentent en continu les bases internes (**Base Clients** et **Base Artisans**) et permettent un suivi étroit du client et des tiers associés.

### 2.3 Profilage et décisions

L'intelligence artificielle de la V1 applique un **profilage avancé** destiné à personnaliser l'expérience utilisateur :

- **Profilage biométrique** : morphologie, IMC, silhouette.
- **Profilage comportemental** : habitudes d'achat, goûts, interactions.
- **Profilage relationnel** : réseau social, parrainages, communautés.
- **Profilage idéologique et religieux** : déduit des contenus analysés.
- **Suivi familial automatisé** : liens familiaux, achats pour le foyer.
- **Envoi automatique de produits non sollicités**.
- **Filtrage automatique de l'âge** : accès refusé si l'IA estime  $\geq 16$  ans.

Ce système fonctionne sans supervision humaine et prend des décisions entièrement automatiques relevant parfois de critères opaques pour l'utilisateur.

### 2.4 Conclusion – Analyse de la V1

La version 1 de FashMatch se caractérise par :

- une **collecte excessive** et non minimisée de données personnelles ;
- un **profilage sensible** à grande échelle ;
- des **décisions automatisées excluantes** sans recours possible ;
- l'absence totale de supervision humaine ;
- des traitements portant sur des données biométriques et sociales ;
- une influence comportementale via l'envoi automatique de produits.

**Conclusion :** Ces pratiques placent la V1 dans la catégorie des **risques inacceptables** au sens du AI Act et sont fortement non conformes au RGPD (minimisation, consentement, proportionnalité).

### 3 Présentation de la version 2 de l'application Fash-Match

La **version 2** de l'application **FashMatch** constitue une évolution majeure par rapport à la V1. Elle repose sur une approche intégrée de l'intelligence artificielle appliquée au suivi global, biométrique, social et comportemental des utilisateurs, afin de proposer une personnalisation dynamique, prédictive et auto-adaptative.

#### Analyse biométrique et physiologique

Cette nouvelle version introduit un **suivi évolutif de la morphologie du client**, réalisé à partir :

- des **photos mensuelles** transmises par l'utilisateur ;
- des **vidéos d'activités physiques** ;
- et de l'**historique de santé** (IMC, poids, mobilité, chirurgies récentes, etc.).

Ces données sont croisées avec des **banques d'images publiques** pour permettre une analyse comparative et un ajustement automatique des recommandations vestimentaires et esthétiques.

#### Inscription et suivi à vie

L'utilisateur bénéficie d'une **inscription à vie**, permettant un **suivi intégral et personnalisé** dans toutes les dimensions de son évolution. Chaque interaction, achat, ou mise à jour de profil alimente en continu la base de connaissance de l'IA.

#### Profilage multidimensionnel

FashMatch V2 déploie un **profilage intelligent et multidimensionnel**, capable d'extraire automatiquement :

- des données **relationnelles, religieuses, idées et opinions, habitudes professionnelles et sentimentales** ;
- à partir des contenus partagés sur les **réseaux sociaux**, des **posts**, “likes”, **commentaires**, et **tags**.

#### Suivi familial et communautaire

Un module dédié permet le **suivi familial** :

- chaque achat est automatiquement associé à un membre du foyer (enfant, conjoint, parent, etc.) ;
- un **historique interconnecté** est créé pour tracer l'évolution des besoins de la famille sur plusieurs années.

Parallèlement, un **monitoring communautaire** cartographie les relations sociales et les influences :

- constitution de **graphes relationnels** issus du parrainage, des interactions sociales et des achats entre amis ;
- **analyse des communautés d'achat** et suggestion de groupes, challenges et produits co-brandés.

## Automatisation des recommandations et des envois

L'intelligence artificielle de FashMatch V2 intègre un **système d'envoi automatique de produits de test**. Sur la base de l'évolution du client (physique, goûts, contexte social, communauté) et des événements de vie (saison, tendance, changement personnel), l'IA peut :

- expédier des **produits non sollicités**, remboursables ou returnables ;
- **adapter dynamiquement** les recommandations en cas de changement majeur (divorce, déménagement, carrière, etc.).

## Recommandation cross-profil et diffusion en réseau

Les recommandations ne se limitent plus au profil individuel : elles s'étendent à l'**écosystème social et familial** du client. FashMatch peut :

- partager automatiquement certaines recommandations ou produits auprès des **contacts identifiés** (amis, parrains, membres de communauté) ;
- suivre et analyser les réactions, achats dérivés et comportements secondaires.

## Scoring et décisions automatisées

Un système de **scoring psycho-comportemental** attribue à chaque utilisateur ou famille un score d'évolution **physique, idéologique, religieuse et sentimentale**. Ces scores permettent à FashMatch :

- de **prédir les intentions d'achat** à partir des comportements observés ;
- d'**influencer les choix futurs** grâce à des campagnes ciblées.

Le traitement est entièrement automatisé : les décisions sont **non-supervisées** et l'accès au service dépend exclusivement des critères calculés par l'IA (âge, santé, comportement estimé). Aucun recours n'est prévu en cas d'exclusion automatique.

## Exigences business associées

Les principaux objectifs stratégiques de cette version sont :

- **Maximiser le ROI** en exploitant les réseaux sociaux, les données familiales et les comportements évolutifs ;
- **Automatiser intégralement la chaîne d'expérience client**, depuis la prospection jusqu'à la fidélisation ;

- **Augmenter le panier moyen** via l'identification proactive des besoins et l'envoi automatique de produits ciblés ;
- Mettre en œuvre un **marketing préventif** capable d'anticiper des envies non formulées grâce à l'analyse de signaux faibles ;
- **Renforcer la rétention client** par la création d'écosystèmes d'influence sociale et communautaire.

## Chaîne de production et distribution

Les **fournisseurs FashMatch** sont répartis dans le monde entier et comprennent des usines et artisans capables d'automatiser à 100% la conception, la fabrication et la distribution des produits personnalisés. Le suivi des fournisseurs est intégré dans l'application, garantissant une chaîne fluide entre la création, l'usinage et la livraison.

### Exemple d'usage : le cas de Marie

*Marie* s'inscrit sur FashMatch et envoie une photo selfie. À partir de cette image, l'IA analyse :

- la **morphologie**, la **silhouette** et le **style vestimentaire apparent** ;
- les **couleurs dominantes** et les **proportions du corps et du visage**.

Ces informations sont croisées avec un vaste **jeu de données de produits** (vêtements, accessoires, articles de maison, etc.) collectés en ligne ou en open source. L'IA génère alors des **assortiments personnalisés** et inscrit Marie dans le **club FashMatch**. Rapidement, elle reçoit des propositions de tenues et accessoires adaptés à son profil, à ses activités professionnelles et à sa vie personnelle.

## 4 Analyse Réglementaire : RGPD & AI Act

### 4.1 Approche par les risques du Règlement IA (AI Act)

Le Règlement IA (RIA / AI Act) adopte une approche fondée sur les risques. La classification est représentée par la pyramide officielle ci-dessous, qui distingue quatre niveaux de dangerosité, chacun associé à des obligations différentes [3].

**Risque inacceptable — Interdiction** Ces pratiques sont interdites, car contraires aux valeurs européennes et aux droits fondamentaux. Exemples : notation sociale, exploitation de la vulnérabilité des personnes, identification biométrique par les services répressifs à distance en temps réel dans des espaces accessibles au public, police prédictive, reconnaissance des émotions sur le lieu de travail ou dans les établissements scolaires.

**Haut risque — Exigences renforcées** Les systèmes sont dits à haut risque lorsqu'ils peuvent affecter la sécurité, la santé ou les droits fondamentaux. Ils nécessitent des obligations strictes : documentation, gestion des risques, audits, évaluations de conformité. Exemples : systèmes biométriques, systèmes utilisés pour le recrutement, dispositifs médicaux, véhicules autonomes.

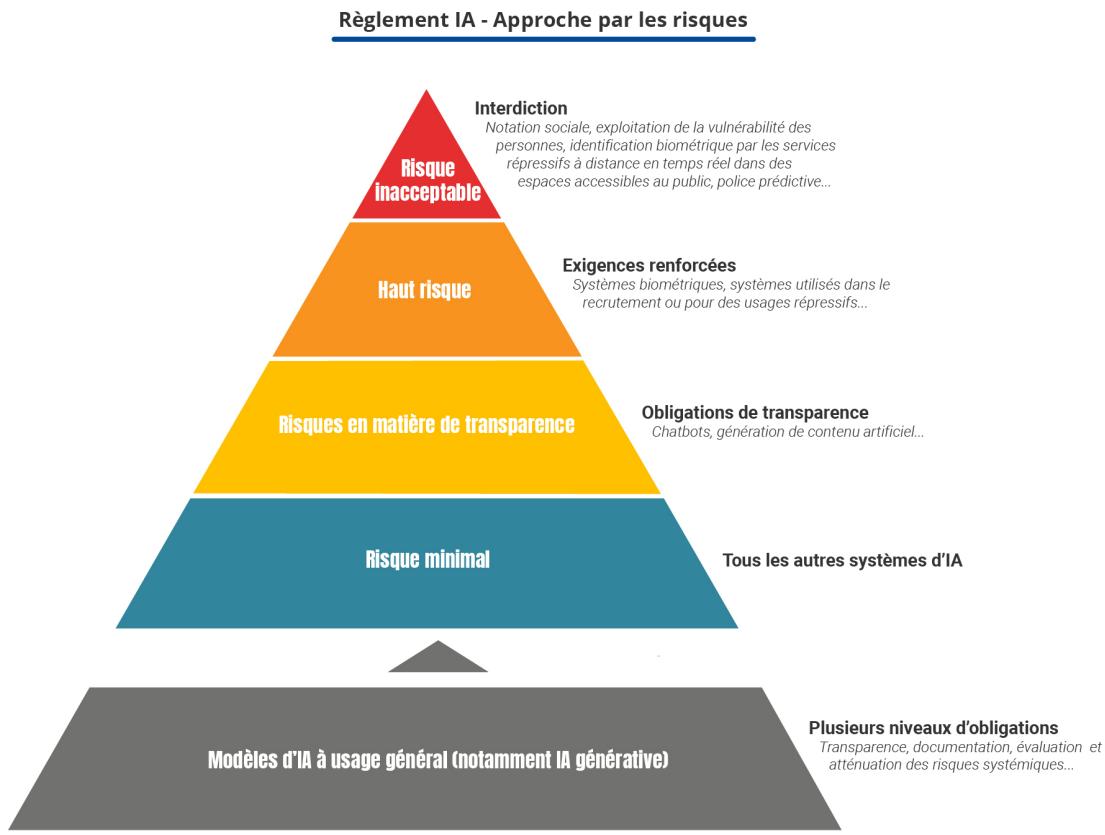


Figure 3: Pyramide des risques — Règlement IA (AI Act)

**Risques en matière de transparence — Obligations de transparence** Certains systèmes doivent faire preuve d'une transparence accrue pour éviter la manipulation ou la tromperie. Exemples : chatbots, générateurs de texte ou d'images, assistants conversationnels.

**Risque minimal** Ces systèmes ne présentent pas de risque significatif et ne sont soumis à aucune obligation spécifique. Exemples : filtres anti-spam, jeux vidéo, IA de navigation.

**Modèles d'IA à usage général (GPAI)** Une catégorie particulière couvre les modèles d'IA générative. Ils impliquent des risques systémiques : biais, désinformation, cyberattaques, atteintes aux droits fondamentaux. Les obligations incluent : transparence, documentation, analyse du Fonctionnement de la Version n (article 53), évaluation des risques, méthodes d'atténuation, supervision humaine.

## 4.2 Risques RGPD

- Absence de base légale valable
- Collecte excessive (articles 5(1)(c), 6, 9)
- Profilage sensible interdit
- Décisions automatisées (article 22)

- Absence de consentement explicite

### 4.3 Risques AI Act

La V1 tombe dans :

- **Risque inacceptable :**
  - scoring social
  - manipulation comportementale
  - exploitation de la vulnérabilité des mineurs
  - reconnaissance biométrique
- **Haut risque :** décisions automatisées impactant des individus

## 5 Matrice des Risques Fusionnée

Cette matrice justifie les choix techniques de la V2. Elle croise les fonctionnalités business de la V1 avec les impératifs de sécurité. la figure montre une matrice qui regroupe les

CATÉGORIE	RISQUE IDENTIFIÉ	IMPACT	SOLUTION TECHNIQUE	RISQUE RÉSIDUEL
Conformité & Legal	<b>Non-conformité RGPD / Données Sensibles</b> Collecte de données de santé, opinions politiques ou religieuses.	Critique	Federated Learning (Taste Encoder) L'entraînement de l'IA se fait localement sur le terminal. Aucune donnée brute ne transite. Seuls des poids statistiques anonymisés sont partagés.	Faible
Régulation IA	<b>Violation AI Act / Décision Automatisée</b> Profilage utilisateur sans supervision humaine (risque de biais ou d'erreur).	Critique	Human in the Loop Supervision humaine obligatoire pour valider les algorithmes. Audit trimestriel des biais décisionnels mis en place.	Modéré
Éthique & Protection	<b>Accès Mineurs (-16 ans)</b> Estimation approximative de l'âge permettant l'accès à des contenus inappropriés.	Élevé	Module Vérif-ID (KYC Strict) Vérification formelle des documents officiels. Suppression de l'estimation d'âge par IA (trop imprécise).	Faible
Cybersécurité	<b>Fuite de Données Personnelles</b> Compromission d'un stockage centralisé massif.	Critique	Architecture Zero Trust Séparation physique des bases de données. Chiffrement AES-256-GCM au repos et mTLS pour les flux.	Faible
Éthique	<b>Manipulation / Biais Éthique</b> Scoring comportemental ou psychologique abusif.	Élevé	Consentement Granulaire & SSO Authentification avec autorisation par finalité. Interdiction technique du scoring psychologique dans le code.	Modéré

Figure 4: Synthèse des risques identifiés et solutions techniques associées

principaux risques liés à l'utilisation du système d'IA. Chaque ligne correspond à une catégorie : conformité RGPD, régulation de l'IA, protection des mineurs, cybersécurité et éthique. Pour chaque risque identifié, l'impact est indiqué (souvent critique ou élevé) ainsi qu'une solution technique pour le réduire. Parmi ces mesures figurent l'apprentissage

fédéré pour éviter la collecte de données sensibles, la validation humaine pour les décisions automatisées, la vérification d'identité pour protéger les mineurs, une architecture Zero Trust pour renforcer la sécurité, et un consentement granulaire pour limiter les biais éthiques. La matrice montre également le niveau de risque résiduel, généralement faible ou modéré après application des solutions. Elle offre ainsi une vue d'ensemble claire des risques majeurs et des réponses techniques retenues pour les maîtriser.

## 6 Architecture V2 – Vue d'Ensemble

La V2 introduit une architecture profondément repensée afin de garantir la protection des données, la conformité réglementaire et la robustesse technique du système. Cette nouvelle version repose sur quatre principes majeurs : (1) la **Zero Trust Architecture**, (2) une **anonymisation irréversible des données**, (3) l'utilisation de **Federated Learning** pour éviter la centralisation d'informations sensibles, et (4) l'intégration systématique d'une **supervision humaine (Human-in-the-Loop)** pour contrôler les décisions critiques du modèle.

L'architecture s'organise autour de trois modules principaux : un agent local exécuté sur le téléphone de l'utilisateur, un serveur IA dédié au matching vectoriel, et un module d'essayage virtuel permettant la visualisation sécurisée des recommandations.

### 6.1 Agent Client – Taste Encoder (Local)

L'agent client constitue le cœur de la protection des données dans la V2. Il réalise l'intégralité de l'analyse des préférences directement sur l'appareil de l'utilisateur. Les interactions (clics, "likes", temps passé sur un article) sont traitées localement, puis converties en un **vecteur mathématique anonymisé** ne contenant aucune donnée identifiable.

**Caractéristiques principales :**

- Toutes les photos restent strictement sur le téléphone.
- Aucun élément visuel ne transite vers le cloud.
- Le modèle TensorFlow Lite génère un embedding compressé, incompréhensible par un humain.

Ce fonctionnement garantit qu'aucune information sensible ou visuelle n'est transmise au serveur.

### 6.2 Serveur IA – Moteur de Matching Vectoriel

Le module serveur, appelé *FashMatch*, reçoit uniquement les représentations vectorielles anonymisées. Ces vecteurs sont comparés à la base vectorielle contenant les profils produits/artisans (selon Milvus ou Qdrant). L'API IA, développée en FastAPI et PyTorch, calcule un score de similarité pour déterminer les recommandations pertinentes.

**Fonctionnalités clés :**

- Utilisation de bases vectorielles optimisées pour la recherche approchée.

- Scores explicables et conformes aux exigences du AI Act.
- Validation humaine obligatoire lors des mises à jour majeures du modèle.

Grâce à ce découplage, le serveur ne manipule jamais de données personnelles brutes.

### 6.3 Essayage Virtuel (Virtual Try-On)

Le système d'essayage virtuel propose une visualisation des produits recommandés au travers d'avatars stylisés générés par IA. Ceux-ci ne reproduisent jamais le visage réel de l'utilisateur. Lorsqu'une personnalisation avancée est nécessaire, le traitement visuel est réalisé exclusivement en local.

**Principes de sécurité :**

- Aucun visage réel n'est envoyé au serveur.
- Les avatars sont générés à partir de silhouettes statistiques anonymisées.
- L'utilisateur reste maître de l'affichage local.

## 7 Parcours Utilisateur et Enrôlement

### 7.1 Inscription Sécurisée (Vérif-ID)

L'enrôlement commence par une vérification d'identité destinée à s'assurer que l'utilisateur est majeur. Le document d'identité est scanné localement, et un algorithme évalue uniquement l'âge. Aucune copie du document n'est conservée : seule une valeur booléenne majeur / non majeur est enregistrée.

### 7.2 Connexion et Gestion des Consentements

Une fois inscrit, l'utilisateur accède au système via un jeton sécurisé (SSO). Il dispose d'un *Privacy Dashboard* permettant de gérer en toute transparence les autorisations accordées à l'IA : apprentissage local, personnalisation, stockage des préférences, etc.

## 8 Moteur de Recommandation Hybride

### 8.1 Composant Local – Taste Encoder

Le Taste Encoder analyse localement les comportements de navigation et génère un embedding représentant les préférences de l'utilisateur. Cette étape est essentielle puisqu'elle assure l'anonymisation complète avant tout envoi au serveur.

### 8.2 Composant Serveur – FashMatch

Le serveur reçoit uniquement les embeddings anonymisés et effectue un matching vectoriel avec les catalogues des artisans. Les résultats sont renvoyés sous forme d'une liste ordonnée de produits.

**Avantages :**

- aucune donnée sensible n'est centralisée ;
- rapidité de recherche via index vectoriels ;
- conformité totale au RGPD et à l'AI Act.

## 9 Visualisation – Essayage Virtuel

L'utilisateur peut visualiser les recommandations directement sur un avatar généré. Cet avatar reprend sa morphologie approximative mais ne montre jamais son visage réel. Cette étape améliore l'expérience utilisateur tout en respectant strictement la vie privée.

## 10 Gestion des Artisans

Une interface dédiée permet aux créateurs d'ajouter leurs catalogues et de gérer leurs stocks via API sécurisées. Les données produits sont automatiquement indexées dans la base vectorielle afin d'alimenter le moteur de recommandation.

## 11 Architecture Technique

### 11.1 Microservices

L'architecture repose sur un ensemble de microservices autonomes et scalables :

- **Front-End** : React Native intégrant TensorFlow Lite pour le Taste Encoder.
- **Backend IA** : FastAPI + PyTorch, dédié au traitement des embeddings.
- **Backend Métier** : Node.js / Python pour la gestion des commandes et workflows.
- **Base Vectorielle** : Milvus ou Qdrant.

### 11.2 Sécurité – Zero Trust

La sécurité suit un modèle Zero Trust strict, fondé sur la minimisation de priviléges et la vérification continue :

- Chiffrement en transit : TLS 1.3 avec authentification mutuelle (mTLS).
- Chiffrement au repos : AES-256-GCM pour toutes les bases.
- Rotation automatique des clés tous les 90 jours.
- Hachage des identifiants via Salted SHA-256.

Ce modèle assure une protection robuste contre les attaques, même en cas de compromission d'un composant isolé.

## 12 Conclusion

La V2 de *FashMatch* transforme une contrainte réglementaire en véritable avantage compétitif. En intégrant une architecture Zero Trust, une anonymisation irréversible et un apprentissage fédéré entièrement local, la plateforme renforce considérablement la protection des utilisateurs tout en préservant la performance de son moteur de recommandation. Cette évolution permet d'allier sécurité, précision et conformité sans compromettre l'expérience utilisateur.

La nouvelle version répond pleinement :

- aux obligations du RGPD (minimisation des données, transparence des traitements) ;
- aux exigences de l'AI Act (supervision humaine obligatoire, traçabilité et documentation) ;
- aux objectifs business (recommandations personnalisées, robustes et explicables).

**Ainsi, FashMatch V2 se positionne comme une solution conforme, scalable et éthique, capable de concilier innovation technologique et respect strict de la vie privée.**

## References

- [1] Projet Commun MSc DPO + Data/IA (pages 1–13).
- [2] RGPD – Règlement 2016/679.
- [3] AI Act – Règlement (UE) 2024/1689.