



La grande école du numérique pour tous

# Audit de conformité Projet FashMatch

DPO – Data/IA  
Di Landro Thomas  
Skander Saadoune  
Mohamed Ahmedvall

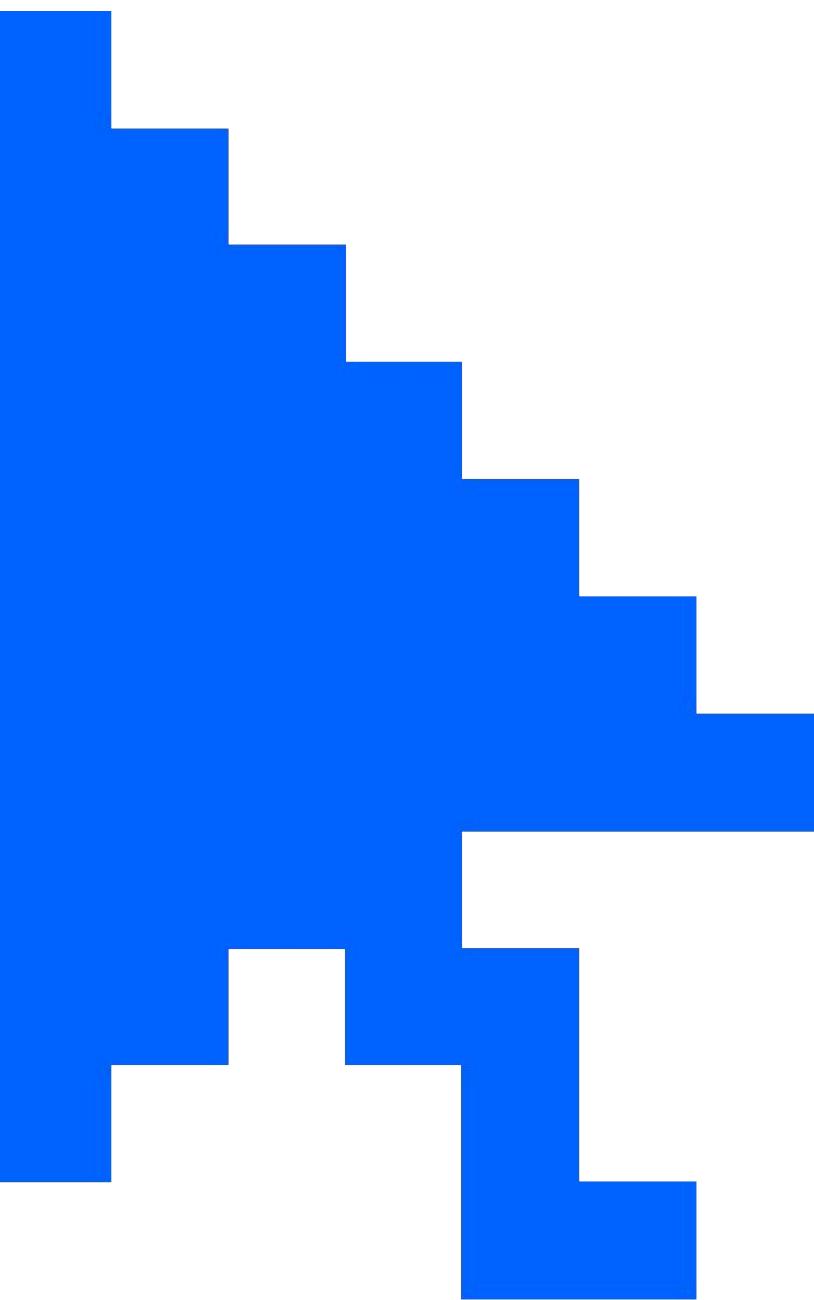


# Contexte et Périmètre

## Le Projet FashMatch

Plateforme combinant personnalisation vestimentaire et IA générative.

L'objectif est de fournir des recommandations basées sur la morphologie et le style.



## Objectif de l'Audit DPO

- Analyser les traitements de données.
- Vérifier la conformité.
- Se conformer au règlement IA Act
- Identifier les risques critiques pour les utilisateurs.

# Cartographie des Traitements

## Fonctionnement

T1: Gestion des comptes

T6: Base clients/artisans

T11: Traçabilité production

Traitements classiques de gestion de service

## Personnalisation

T3: Profilage comportemental

T5:  
Recommandations produits

T8: Entraînement modèles IA

T10: Tests produits

## Traitements Sensibles

T2: Biométrie

T4: Scoring

Psycho-comportemental

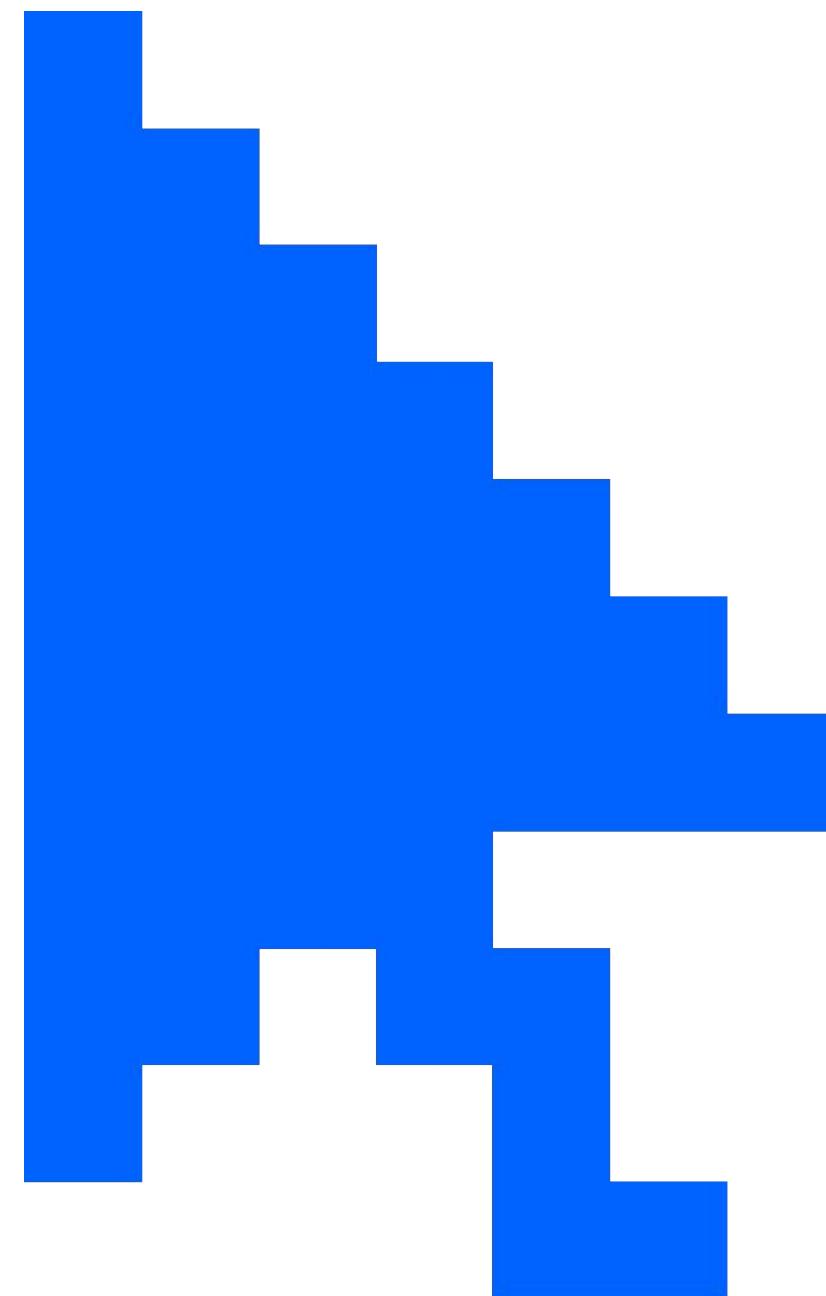
T9: Graphes d'influence

Risques majeurs identifiés.

# Analyse RGPD : Les Non-Conformités

## **Manque de Transparence (Art. 12-14) :**

Aucune information claire sur l'usage des données ou les bases légales.



## **Consentement Absent (Art. 6 & 9) :**

Collecte de données biométriques sans consentement explicite.

## **Décisions Automatisées (Art. 22) :**

Refus d'accès et scoring sans intervention humaine ni recours possible.

## **Minimisation des Données (Art. 5) :**

Collecte excessive d'informations sociales et familiales pour un simple service vestimentaire.

## **Sécurité (Art. 32) :**

Aucune mesure technique documentée dans le prototype initial pour protéger les données sensibles.

# Analyse IA Act : Haut Risque & Interdits

## HAUT RISQUE

### T2 : Biométrie

Filtrage âge/morphologie

Action requise :

Ajout d'une supervision

humaine effective et d'un

consentement explicite

obligatoire.

## PRATIQUE INTERDITE

### T4 : Scoring Psycho

Scoring  
comportemental &  
social

Action requise :

Suppression totale du  
module de scoring.

## HAUT RISQUE

### T9 : Graphes Sociaux

Suivi communautaire

Action requise :

Anonymisation irréversible

des graphes, audit

anti-biais et droit

d'opposition (Opt-out).

# Synthèse des Risques Majeurs

## Manque de Transparence

L'utilisateur ignore tout du traitement de ses photos et du calcul de ses scores. Un "effet boîte noire" contraire à l'Art 13 du RGPD.

## Décisions Automatisées

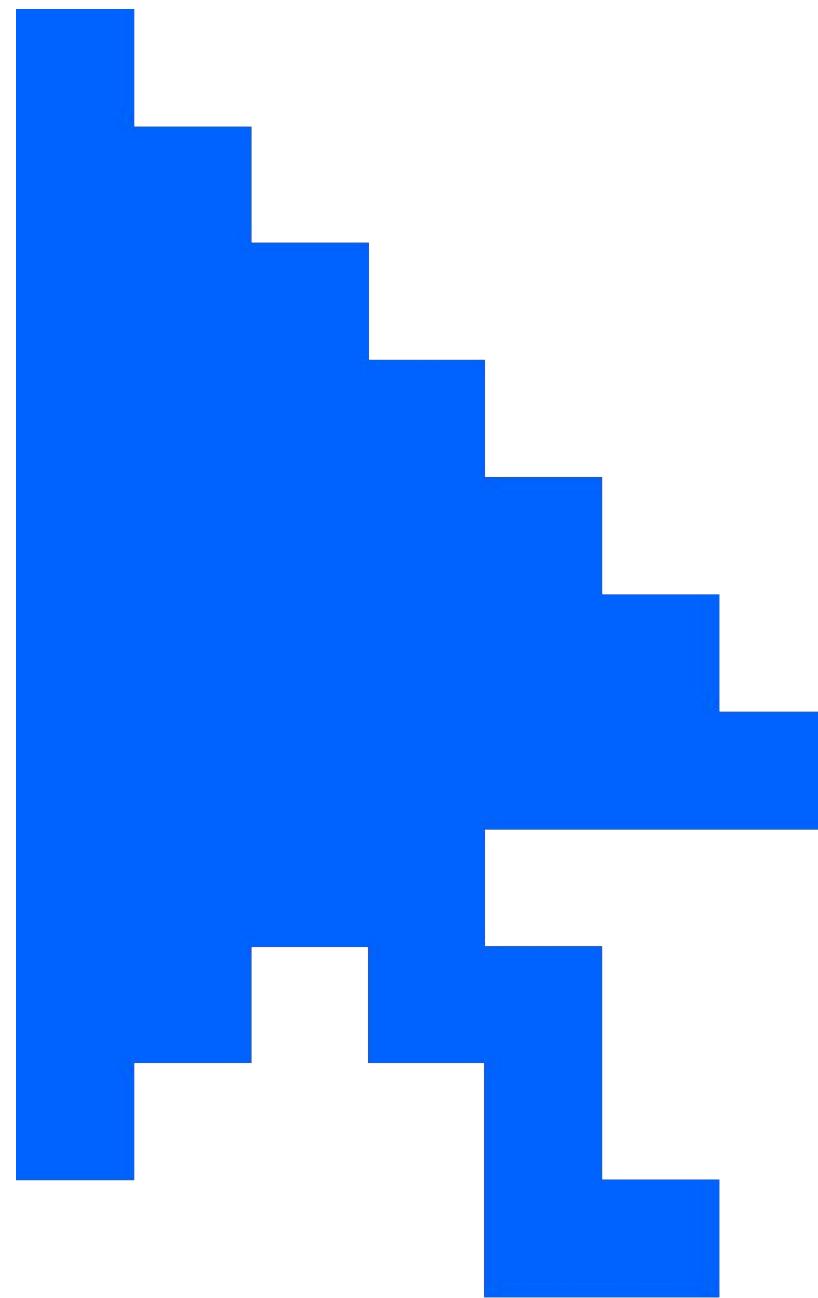
Impact juridique direct (refus d'accès, classement) sans aucune validation humaine, violent l'Art 22 du RGPD et l'IA Act.

## Profilage Excessif

Combinaison de données physiques, sociales et comportementales créant un profilage intrusif disproportionné par rapport à la finalité.

## Scoring Social

Risque critique de discrimination via des scores de comportement/influence non expliqués, pratique interdite par l'IA Act.



# Mesures de Conformité Proposées

## Juridique & Gouvernance

- **Mise à jour Documentation** : Réécriture complète Politique de Confidentialité & CGU (Art 13/14).
- **Registre (Art 30)** : Création des fiches pour les traitements T1 à T11.
- **Sous-traitants** : Audit des contrats éventuels et ajout des clauses RGPD, IA ACT.

## Droits des Personnes

- **Consentement** : Module de recueil explicite "Opt-in".
- **Centre de Contrôle** : Dashboard utilisateur pour gérer ses données (Droit d'accès/Portabilité).
- **Droit à l'humain** : Procédure d'escalade pour contester une décision algorithmique (Art 22).
- **Mineurs** : Verrouillage spécifique pour les -15 ans (consentement parental).

## Privacy by Design

- **Minimisation** : Purge automatique des données brutes après analyse.
- **Anonymisation** : Techniques de "Privacy Preserving ML" pour l'entraînement des modèles.
- **Sécurité** : Chiffrement AES-256 au repos et TLS 1.3 en transit.
- **Auditabilité** : Logs de toutes les actions d'administration.

# Plan d'Action

## Immédiat

### Priorité Critique

Mise en conformité Biométrie (T2) et Scoring (T4). Intégration du consentement et supervision humaine.

## Moyen Terme

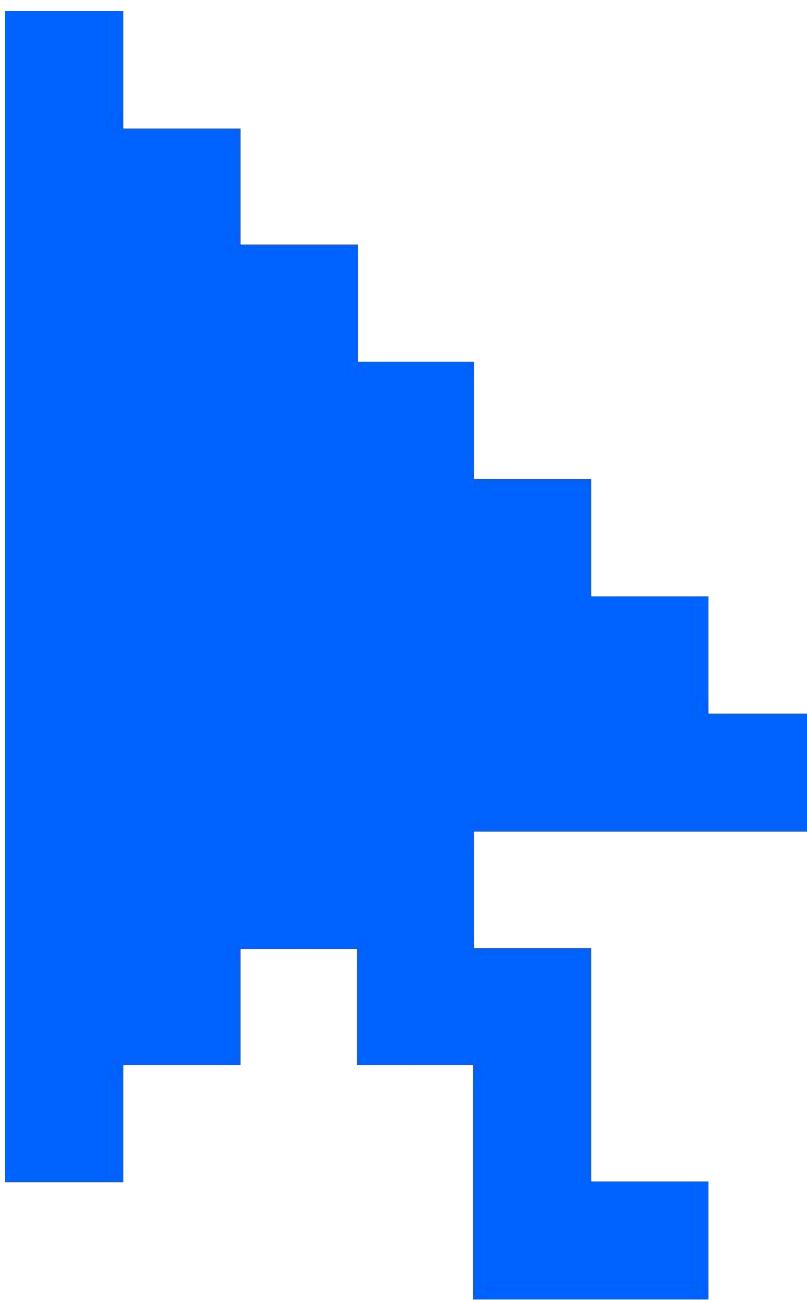
### Sécurité & Socle

Déploiement chiffrement, pseudonymisation, logs.

## Long Terme

### Prêt pour l'IA Act

Documentation technique complète, audit régulier des biais.



# Conclusion de la DPO

## Diagnostic ambivalent :

Une excellence technique indéniable, mais une conception initiale ignorant la vie privée (*Privacy by Design* absente).

## Risque critique (Go/No-Go) :

Mise en production impossible en l'état sous peine de sanctions massives (7% du CA mondial via l'AI Act).

## Plan de remédiation :

Application immédiate des mesures correctives (transparence, arrêt du scoring toxique, supervision humaine).

## Objectif final :

Transformer une "boîte noire" risquée en une plateforme éthique, robuste et de confiance.

Cahier des Charges Final

# FashMatch V2

Conformité RGPD, AI Act et Architecture Data/IA

---

**Projet :** À la croisée des Arts

**Auteur :** Mohamed/Skander



# Contexte et Pivot Stratégique

---



## Vision Initiale (V1)

FashMatch V1 reposait sur un modèle de "Personal Shopper" intrusif :

- Collecte massive et non minimisée de données.
- Profilage psychologique et biométrique agressif.
- Objectif purement commercial : maximisation du profit par l'influence comportementale.



## Nouvelle Vision (V2)

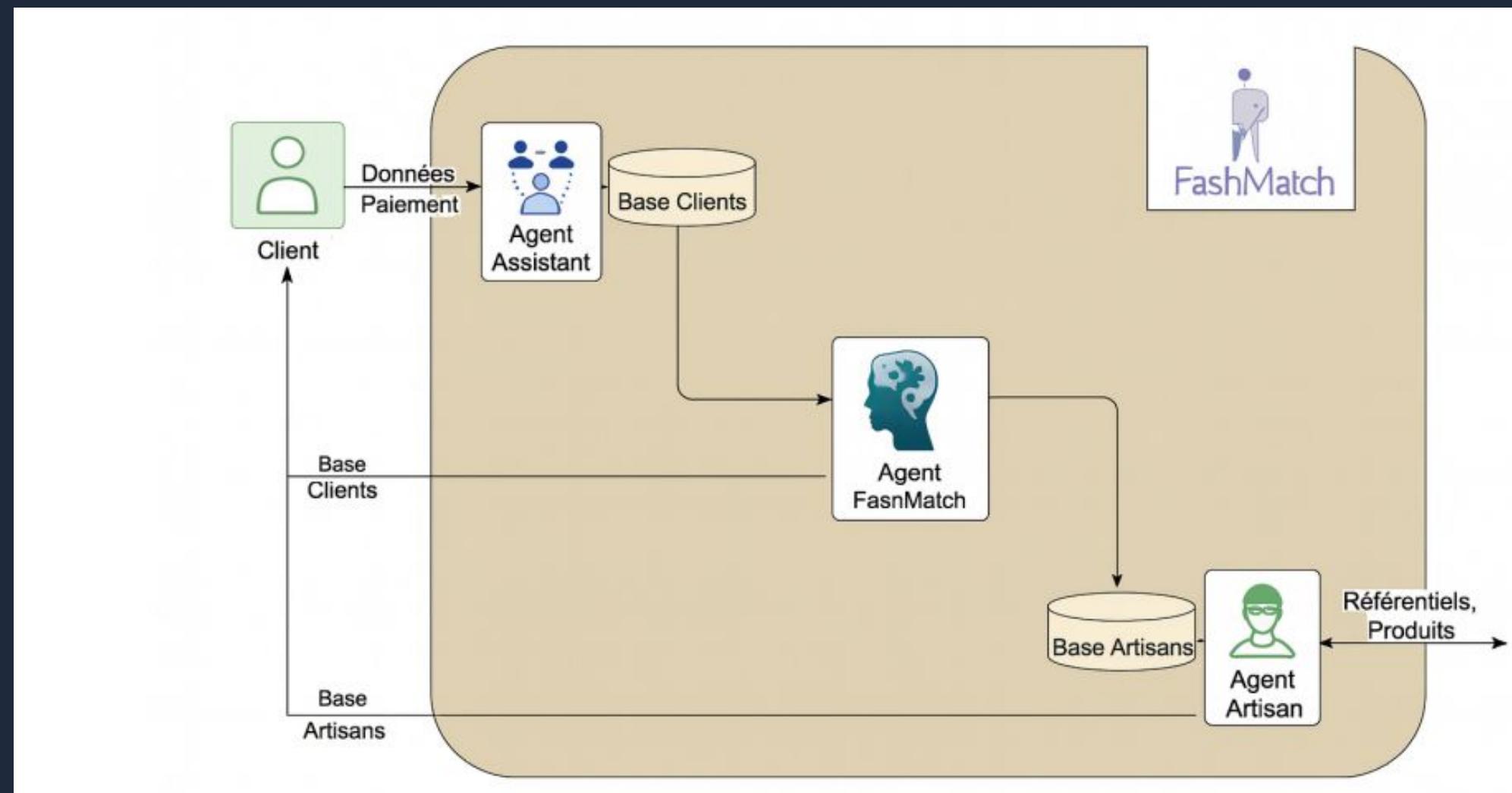
Le pivot vers la V2 vise une conformité totale et éthique :

- Architecture **Zero Trust** et Privacy-by-Design.
- Respect strict du RGPD et du AI Act (UE).
- Maintien de la personnalisation via l'IA locale (Edge AI) et l'anonymisation.

# Analyse V1 : Une Approche Risquée

La version initiale centralisait un volume excessif de données sensibles, créant une surface d'attaque critique :

- ✓ **Biométrie** : Photos, vidéos, morphologie, IMC.
- ✓ **Vie Privée** : Données familiales, opinions politiques/religieuses déduites.
- ✓ **Comportement** : Suivi social, analyse sentimentale.
- ✓ **Décisions** : Envois automatiques de produits non sollicités et filtrage opaque des utilisateurs.



# Risques Critiques V1

---

## Risques Inacceptables (AI Act)

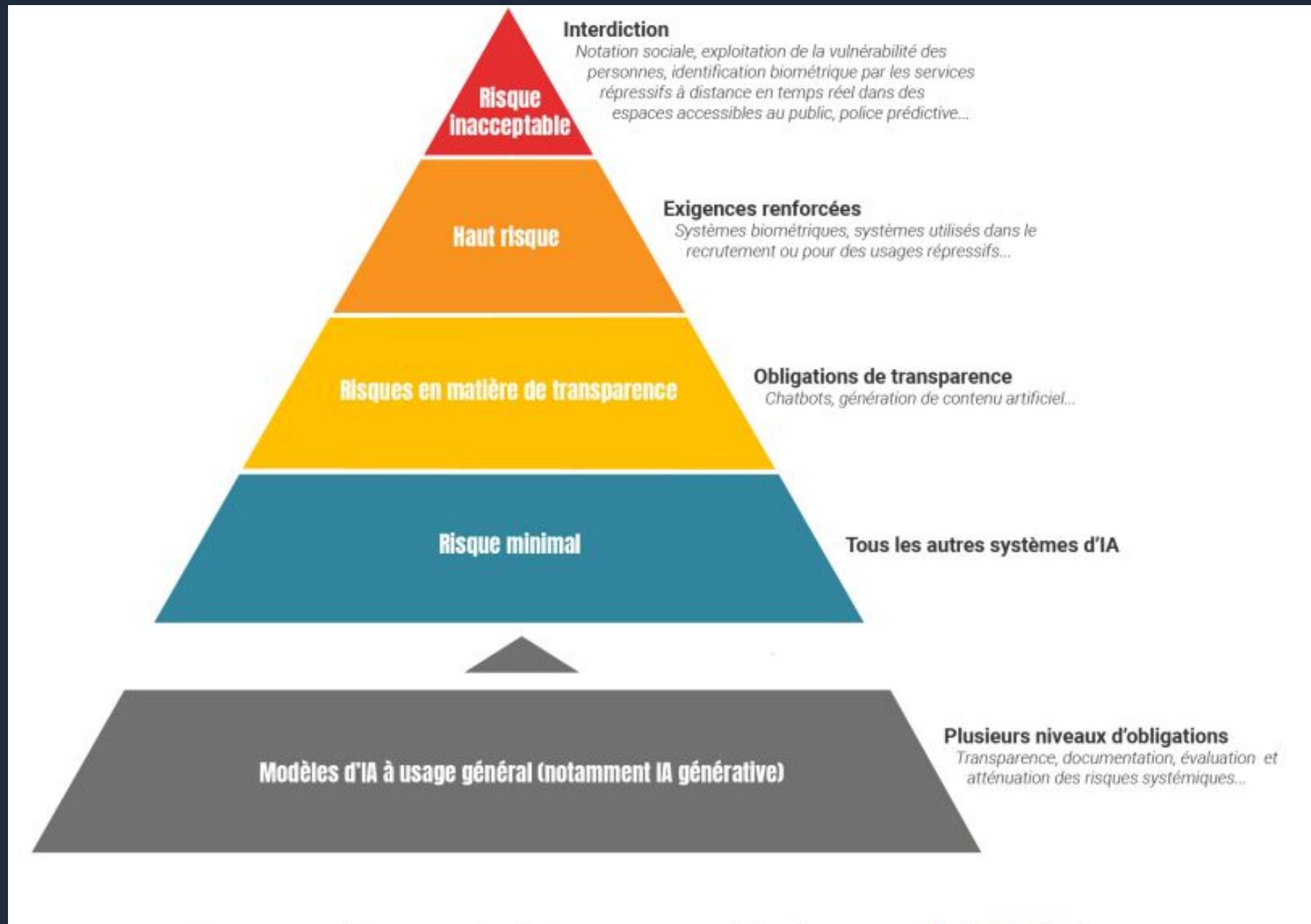
La V1 entre dans la catégorie "Interdite" :

- Scoring social et manipulation comportementale.
- Exploitation de la vulnérabilité des personnes (mineurs).
- Identification biométrique à distance.

## Violations RGPD

- Absence de consentement libre et éclairé.
- Non-respect du principe de minimisation.
- Profilage sensible illicite.

# Cadre Réglementaire : AI Act



## L'Approche par les Risques

Le règlement européen classe les systèmes IA en 4 niveaux :

- ✓ **Risque Inacceptable** : Interdiction totale (ex: Social Scoring de la V1).
- ✓ **Haut Risque** : Exigences strictes de conformité, sécurité et supervision humaine (Cible pour certaines briques V2).
- ✓ **Risque Limité** : Obligations de transparence (Chatbots, interaction humaine).
- ✓ **Risque Minimal** : Aucune restriction majeure.

# Architecture Cible V2 : Privacy First

---



## Zero Trust

Aucune confiance implicite.  
Authentification forte (mTLS) et  
chiffrement systématique  
(AES-256) pour chaque  
microservice.



## Federated Learning

L'apprentissage se fait  
localement. Les données brutes  
ne quittent jamais l'appareil de  
l'utilisateur.



## Anonymisation

Transformation des données  
personnelles en vecteurs  
mathématiques irréversibles pour  
le matching.

# Fonctionnement Hybride V2

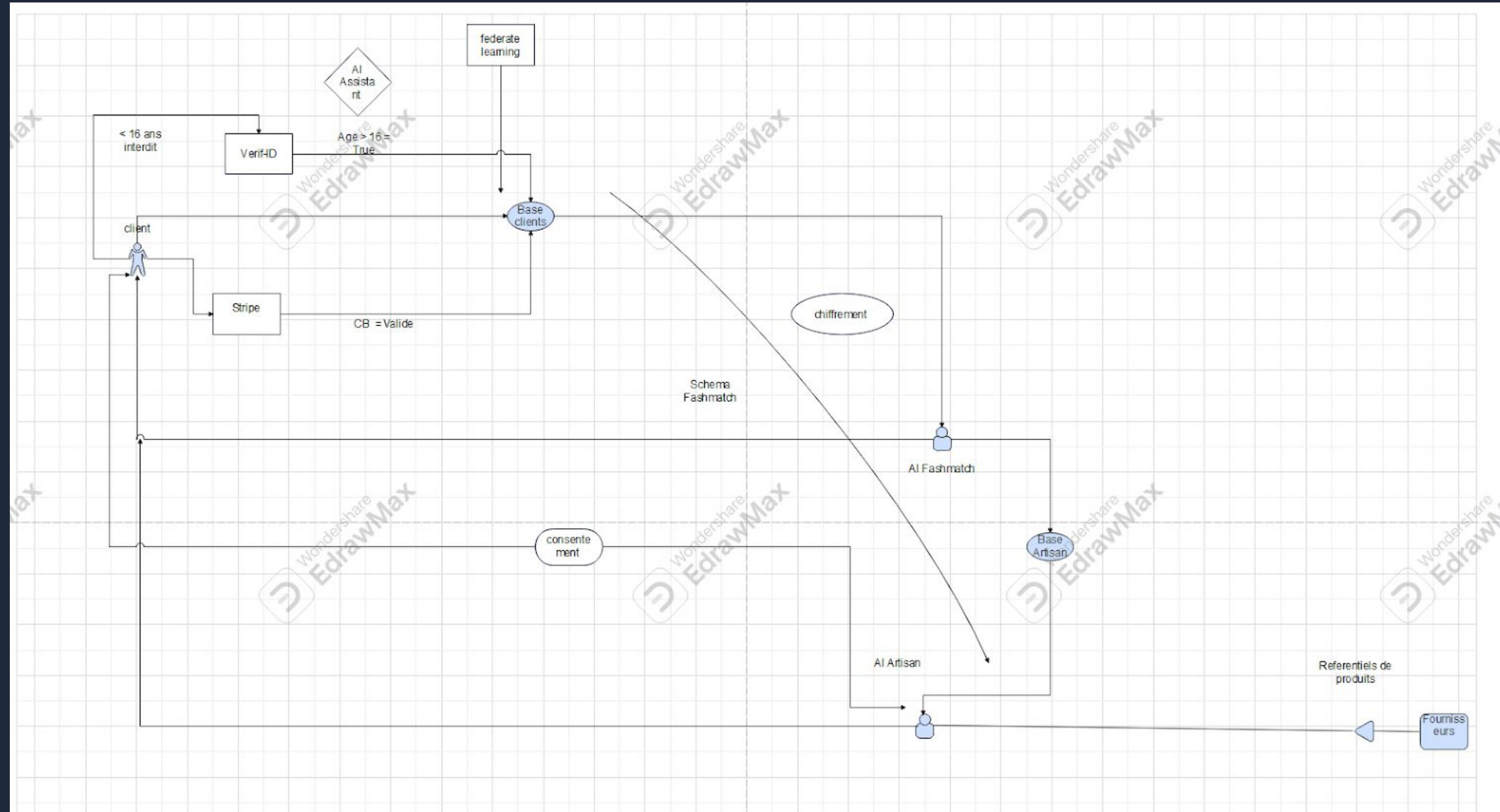
## 1. Agent Client (Local)

Le "Taste Encoder"

## 2. Serveur Vectoriel (Cloud)

(Milvus/Qdrant)

# Architecture cible V2



# Stack Technique & Sécurité

---



## Microservices

- ✓ **Front** : React Native + TensorFlow Lite (Local).
- ✓ **Backend IA** : Python (FastAPI, PyTorch).
- ✓ **DB Vectorielle** : Milvus ou Qdrant.
- ✓ **Business** : Node.js.



## Sécurité Avancée

- ✓ **Chiffrement** : AES-256-GCM pour les données au repos.
- ✓ **Transport** : TLS 1.3 obligatoire.
- ✓ **Gestion des clés** : Rotation tous les 90 jours.
- ✓ **Hachage** : Salted SHA-256 pour les identifiants.

# Matrice de Gestion des Risques

CATÉGORIE	RISQUE IDENTIFIÉ	IMPACT	SOLUTION TECHNIQUE	RISQUE RÉSIDUEL
Conformité & Légal	<b>Non-conformité RGPD / Données Sensibles</b> Collecte de données de santé, opinions politiques ou religieuses.	Critique	<b>Federated Learning (Taste Encoder)</b> 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	<b>Human in the Loop</b> 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	<b>Module Vérif-ID (KYC Strict)</b> 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	<b>Architecture Zero Trust</b> 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	<b>Consentement Granulaire &amp; SSO</b> Authentification avec autorisation par finalité. Interdiction technique du scoring psychologique dans le code.	Modéré

# Spécifications Fonctionnelles Clés

---

## Enrôlement

Vérification d'identité obligatoire pour protéger les mineurs.  
Dashboard de gestion des consentements accessible à tout moment.

## IA Responsable

Explicabilité des recommandations. L'utilisateur doit comprendre pourquoi un article lui est proposé (XAI).

## Supervision

Mécanisme de recours humain en cas de contestation d'une décision ou d'un blocage de compte.

# Conclusion

FashMatch V2 transforme une contrainte réglementaire en avantage compétitif.



Conforme  
RGPD



Compatible AI  
Act



Éthique &  
Scalable

# Questions ?

Merci de votre attention.

LesZétrangers