Analyse d'Impact relative à la Protection des Données (AIPD)

Projet : FashMatch V2 (Application de recommandation vestimentaire par IA)

Avertissement

Cette Analyse d'Impact se base sur les spécifications technique du cahier des charges relatif à la v2 de l'application FashMach, proposé par l'équipe des Data/IA et validées par l'audit de conformité. Elle conclut que le traitement, sous réserve du maintien strict des mesures décrites ci-dessous, présente un risque résiduel toujours présent, mais acceptable.

PARTIE 1 : La description du traitement

a) Description générale

FashMatch V2 est une application mobile de "fashion tech" proposant des recommandations vestimentaires personnalisées. Elle s'appuie sur un système hybride d'Intelligence Artificielle pour analyser les préférences stylistiques et la morphologie des utilisateurs.
Classification : Le système est qualifié de **Système d'IA à Haut Risque** au sens de l'AI Act européen (Annexe 3), en raison du traitement de données biométriques et du profilage.

b) Données personnelles collectées

- **Données d'identification :** Nom, prénom, email.
- **Données de vérification d'âge :** Copie de la Carte Nationale d'Identité (CNI). Supprimée immédiatement après vérification.
- **Données biométriques et à caractère sensible :** Photographies (selfie, corps entier) donnés par l'utilisateur.
- **Données de profilage :** Préférences de style, budget, historique d'interactions (likes/rejets), historique d'achats.

c) Finalités du traitement

1. **Finalité Principale :** Fournir des recommandations de produits personnalisées basées sur la morphologie et les goûts.
2. **Finalité Secondaire :** Amélioration du service via l'analyse des interactions (statistiques anonymes).
3. **Finalité de Sécurité :** Vérification de l'âge pour empêcher l'accès aux mineurs de moins de 16 ans.

d) Flux de données

1. **Collecte et Consentement :** L'utilisateur consent explicitement à chaque finalité via

une interface granulaire.
2. **Vérification d'âge (Human-in-the-loop) :** Un opérateur humain vérifie la CNI et valide l'âge. Le fichier CNI est détruit instantanément.
3. **Traitement Local :** Les photos sont analysées **sur l'appareil de l'utilisateur** (ou serveur local sécurisé) par une IA open-source. Elles ne sont jamais envoyées en clair vers le Cloud public.
4. **Envoi Cloud (Pseudonymisation) :** Seul un vecteur mathématique (embedding) abstrait et les préférences textuelles sont envoyés à l'API d'IA (Hébergement UE).
5. **Gestion des droits :** L'utilisateur garde le contrôle via un onglet Privacy (accès, suppression, floutage).

e) Durée de conservation

- **Données de profil :** 3 ans après la dernière activité (purge automatique).
- **Pièce d'identité :** Suppression immédiate post-vérification.

PARTIE 2 : Contrôle de proportionnalité

a) Base légale (RGPD)

- **Traitement général :** Art. 6.1.a (Consentement).
- **Données biométriques (Art. 9) :** Art. 9.2.a (Consentement explicite).
- **Validation Audit :** Le recueil du consentement est libre, spécifique, éclairé et univoque.

b) Proportionnalité des mesures

- **Minimisation :** L'architecture hybride assure que les données les plus intrusives ne quittent pas l'environnement local/maîtrisé. Seules les données strictement nécessaires au matching sont partagées.
- **Maîtrise utilisateur :** Les options de "floutage visage" et d'utilisation d'avatars 3D offrent des alternatives moins intrusives pour le même service.

PARTIE 3 : Matrice de risques Droit et Libertés

Risque Identifié	Gravité Initiale	Mesures de Mitigation (Auditées)	Risque Résiduel
Traitement illicite de données sensibles (Collecte sans base légale)	ÉLEVÉE	• Consentement explicite par moduel. • Architecture Hybride (Traitement local).	FAIBLE
Discrimination / Exclusion (Refus d'accès erroné	ÉLEVÉE	• Suppression de l'IA de vérification d'âge. • Remplacement par	FAIBLE

sur l'âge)		validation humaine.	
Biais algorithmique (Recommandations stéréotypées)	MOYENNE	• Explicabilité des résultats fournie à l'utilisateur.	FAIBLE/MOYEN
Ré-identification	MOYENNE	• Pseudonymisation	FAIBLE/MOYEN
Violation de données (Vol de photos ou profils)	ÉLEVÉE	• Chiffrement • Hébergement Cloud souverain/UE (ISO 27001).	FAIBLE

PARTIE 4 : Synthèse

a) Synthèse des mesures

L'audit de conformité a validé l'effectivité des mesures suivantes :

1. **Organisationnelles :** Validation humaine de l'âge, tenue des registres (RGPD/IA), procédure de gestion des incidents.
2. **Techniques :** Traitement local des données brutes (Privacy by Design), chiffrement de bout en bout, purge automatique.

b) Avis du DPO

Bien que FashMach puisse encore être considéré comme utilisant des système d'IA à haut risque, nécessitant l'information approprié de la CNIL, les risques concernant les droits et libertés des individus ont été très largement amoindris. La double approche mitigation/compliance amène à un résultat ou les risques résiduels sont minimes considérant l'ampleur du niveau de risque initial de FastMach. Enfin, ces effort de mise en conformité ont eu relativement peu d'impact sur le fonds du projet FastMach, bien que des fonctionnalité aient disparues.