Plan de conformité et rapport d’audit

Projet : Transition FashMatch V1 (Non-Conforme) vers V2 (Compliance by Design)

PARTIE I : Le plan d’audit

1. Les objectifs de l’Audit de conformité

Dès le premier coup d’œil, le prototype FashMatch V1 a été identifié comme non conforme à la mise sur le marché (Non-conformité RGPD et AI Act). Ces impressions et premier “réflexes” doivent être approfondis pour ne passer à côté d’une faille plus profonde dans la conception. L’objectif principal est de développer une version de FashMach capable d’intégrer au cœur de son fonctionnement les enjeux éthiques relatifs à la protection des données et aux risques liés à certains systèmes d’intelligences artificielles (En l’espèce, IA à haut risque).
En coordination avec l’équipe Data/IA, le projet initial est immédiatement passé en revu afin d’identifier et de confirmer les indices forts regardant le faible niveau de maturité de FashMach en matière de conformité, et d’en évacuer les points critiques (illégalités et non conformités flagrantes). Dans un deuxième temps, identifier les failles restantes pour produire une V2 "Conforme by design". Objectif de l'audit : valider sous 5 jours que les spécifications (cahier des charges V2) et l'architecture technique suffisent à lever les risques légaux pour pour permettre le déploiement de l’application. Enfin, il s’agira d’assurer la qualité des mesures et alternatives trouvées pendant la première semaine du projet (dédiée à l’Audit), ainsi que de constituer un dossier de livrables démontrant le niveau de conformité avancé de la version 2 de FashMach.

2. Matrice des Risques RIA et RGPD

Le tableau suivant sert de “Matrice de risques” relative à la conformité du produit FashMach et les mesures proposées entre la V1 et la V2 .

Niveau de Risque	Problème V1	Solution V2	Mise en place
CRITIQUE	**Données Sensibles :** Collecte sauvage d'opinions et biométrie.	**Consentement et Pseudonymisation :** Architecture hybride (Local/Cloud) + Consentement explicite.	API Cloud ne recevant *jamais* de données à caractère personnel non pseudonymisées ou données sensibles brutes.
CRITIQUE	**Décision Auto :** Exclusion automatique (âge) sans recours. Détermination automatisée de l'âge de la personne concernée.	**Supervision Humaine :** Vérification Pièce Nationale d'identité, avec "Human-in-the-loop".	Procédure écrite montrant *qui* valide et *comment* on conteste.
ÉLEVÉ	**Transparence :** Utilisateur ignorant le profilage. Pas d'informations relatives au traitement.	**Plateforme "Privacy" :** Interface de gestion des droits (accès/suppression/floutage).	Création d'une interface des droits pour les personnes (floutage, données collectées, avatar virtuel). La personne concernée à un droit direct sur l'activité de traitement de ses données.
ÉLEVÉ	**AI Act :** Absence de gouvernance.	**Documentation :** Registres des traitements et analyse de risques.	Présence physique des registres à jour.

3. Ce que la V2 de FashMach doit impérativement contenir pour garantir sa conformité

Voilà à quoi doit ressembler FashMach dans sa version 2 :

- **Minimisation et consentement :** Collecte sur base du consentement explicite (Article 9.2 et 6.1 du RGPD). Architecture hybride : les données brutes sont traitées en local.

- **"Anonymisation" locale :** Seuls des vecteurs pseudonymisés (données dérivées) sont envoyés au Cloud.

- **Supervision Humaine (Human-in-the-loop) :** Vérification d'âge sur Pièce d'identité, validée par un opérateur humain

PARTIE II : Compte rendu et bilan de l'Audit

Le tableau ci-dessous à pour objet de faire un dernier point avant la l'établissement d'une V2 pour l'application FashMach.

1. Résultats de l'Audit en préparation de la Version 2 de FashMach

Domaine	Promesse V2	Résultat Audit	Statut
Biométrie & Sensible	Architecture Hybride (Local/Cloud)	*l'API reçoit uniquement un vecteur mathématique Pseudonymisé*	✅
Consentement	Consentement explicite & granulaire	*L'écran de consentement est conforme*	✅
Décision Auto	Vérification humaine (Âge)	*Le processus à remplacé le modèle d'IA*	✅
Droits Personnes	Interface de suppression/floutage	*L'utilisateur dispose d'un contrôle flexible concernant la collecte et le traitement de ses données*	✅
Sécurité	Chiffrement & Hébergement UE	*Clés de chiffrement gérées en interne - Autres mesures techniques et organisationnelles*	✅

2. Livrables de démonstration de la mise en conformité

Livrable	Objectif	Statut
Registre de Traitement (RGPD)	Documenter de manière exhaustive toutes les activités de traitement de données personnelles (finalités, catégories de données, destinataires, délais de conservation, mesures de sécurité).	Finalisé
Registre des Systèmes d'Intelligence Artificielle (AI Act)	Identifier et documenter les systèmes d'IA utilisés, en particulier l'IA à haut risque (FashMatch V2), détaillant la conformité aux exigences de l'AI Act (documentation technique, traçabilité, surveillance humaine).	Finalisé
Analyse d'Impact relative à la Protection des Données (AIPD)	Évaluer les risques élevés pour les droits et libertés des personnes concernées liés aux traitements de données, notamment l'utilisation de données sensibles et de l'IA.	Finalisé