MISSION DE RÉFÉRENCE ANONYMISÉE

Note de classification Annexe III & d'écarts Annexe IV

SUJET	TalentFit AI · Série B · Éditeur RH-tech mid-market UE
MISSION	Diagnostic (étendu) · 5 jours ouvrés
RÉDIGÉ PAR	Chiekh Alloul, Partner · Tenth Partner

Ceci est un échantillon anonymisé. Les noms, architectures de modèles, ordres de grandeur et dates ont été modifiés afin de retirer toute information identifiante d'une mission réelle. La structure, la méthodologie et l'analyse sont représentatives du livrable remis aux clients.

SECTION 1

Synthèse

L'ESSENTIEL

01 Les trois systèmes en production de TalentFit AI — mise en relation candidats, résumé de tri, scoring d'entretien structuré — relèvent du règlement IA, classés à haut risque au titre de l'Annexe III §4(a).

02 L'exemption de l'Article 6, paragraphe 3 n'est pas disponible pour les trois systèmes. Le LLM de tri a un argument superficiel pour le §6(3)(a) (tâche procédurale étroite) qui s'effondre du fait du couplage en aval avec le matcher.

03 Sur les dix-huit exigences Annexe IV analysées, onze sont satisfaites ou quasi-satisfaites par des artefacts qui existent déjà dans la stack d'ingénierie. Sept demandent une nouvelle production documentaire.

04 Trois écarts matériels concentrent l'effort de remédiation : aucun plan de surveillance après commercialisation au titre de l'Article 72 ; aucun système de gestion des risques Article 9 documenté ; mesures par sous-groupes calculées dans le pipeline d'entraînement mais non exportées par système livré.

05 L'exposition achats est réelle dès aujourd'hui : deux des comptes grands comptes ciblés par TalentFit AI ont déjà ajouté une section due-diligence règlement IA à leur revue sécurité fournisseur.

> Recommandation : un Sprint de mise en conformité de deux semaines produit la première version du dossier technique à partir des artefacts existants, ainsi que le modèle de SGR Article 9 et une feuille de route à 26 semaines pour l'alignement opérationnel avant le 2 août 2026. Valeur indicative de la mission : 9 500 €.

SECTION 2

Classification Annexe III par système

Chaque système dans le périmètre est évalué au regard de l'Annexe III §4 (emploi, gestion des travailleurs, accès au travail indépendant) et confronté aux quatre exemptions de l'Article 6, paragraphe 3.

Mise en relation candidats (Système 1)

HIGH-RISK

FUNCTION	Classe les candidats face aux postes ouverts via une étape de récupération two-tower suivie d'un reranker à gradient boosté.
I/O	Entrée : caractéristiques candidats et embeddings du descriptif de poste. Sortie : liste ordonnée de candidats avec score de pertinence dans [0, 1] par couple (candidat, poste).
SCALE	Déployé chez environ 150 clients grands comptes ; de l'ordre de 600 000 appels de classement par mois.
ANNEX III PARAGRAPH	Annexe III §4(a) — recrutement et sélection de personnes physiques.
ARTICLE 6(3) ANALYSIS	Non éligible. Le classement façonne matériellement l'attention du recruteur ; les scores de pertinence sont conditionnés par les caractéristiques du candidat (profilage au sens de l'Article 4(4) du RGPD) ; le classement précède toute sélection humaine. Aucun des §6(3)(a)–(d) ne s'applique.

Résumé de tri (Système 2)

HIGH-RISK

FUNCTION	Extrait des signaux structurés à partir de CV en texte libre via un LLM de taille moyenne fine-tuné.
I/O	Entrée : CV en texte libre. Sortie : profil structuré — inventaire de compétences, années d'expérience par domaine, prédiction de séniorité, et résumé d'adéquation au poste en un paragraphe.
SCALE	Environ 4 millions de CV traités sur les 12 derniers mois sur la même base de clients grands comptes.
ANNEX III PARAGRAPH	Annexe III §4(a) — recrutement et sélection.
ARTICLE 6(3) ANALYSIS	Argument superficiel pour le §6(3)(a) — tâche procédurale étroite — car le système effectue une extraction structurée plutôt qu'un scoring substantif. L'argument s'effondre parce que la sortie structurée alimente directement le Système 1 (le matcher) ; l'effet cumulatif est une influence de classement. Le §6(3)(d) — détection d'écart par rapport aux schémas de décision antérieurs — joue également puisque la prédiction de séniorité produite par le LLM peut écraser un tri humain antérieur. Non éligible.

Scoring d’entretien structuré (Système 3)

HIGH-RISK

FUNCTION	Note les réponses d’entretiens vidéo enregistrés au regard d’une grille de compétences, via un classifieur multi-label fine-tuné s’appuyant sur un frontend de speech-to-text.
I/O	Entrée : vidéo et transcription. Sortie : scores par dimension (communication, adéquation au poste, structuration de la pensée) et un score global d’adéquation dans [0, 100].
SCALE	Actuellement en pilote auprès de douze clients grands comptes ; lancement production complet prévu au T3 2026.
ANNEX III PARAGRAPH	Annexe III §4(a) — recrutement et sélection.
ARTICLE 6(3) ANALYSIS	Non éligible. Le scoring est substantif (le modèle évalue directement les candidats à titre individuel) ; aucune exemption pour tâche procédurale ne tient. Le fait qu’un humain examine le score avant de prendre action ne change pas l’analyse — le scoring lui-même est l’acte régulé.

SECTION 3

Analyse d’écarts Annexe IV

Huit exigences représentatives de l’Annexe IV §1, §2 et des Articles opérants, mises en correspondance avec les artefacts d’ingénierie existants de TalentFit AI. La cartographie complète couvre trente lignes et est livrée dans le Sprint.

RÉFÉRENCE	EXIGENCE	STATUT	CRITICITÉ	PREUVE / ÉCART
Annexe IV §1(a)	Identifiant du système et version	✓ Satisfied	–	experiment_id MLflow plus SHA git par modèle livré. Aucun travail requis.
Annexe IV §1(c)	Description de l’interaction du système avec le matériel et les logiciels	◐ Partial	MEDIUM	Schémas d’architecture des services existants pour chaque système dans le wiki d’ingénierie ; aucun document mis en forme Annexe IV. Une journée de rédaction comble l’écart.
Annexe IV §1(g)	Journaux de validation et de tests, signés et datés	◐ Partial	MEDIUM	Historique d’exécutions MLflow et rapports W&B exhaustifs ; discipline de signature et datation manquante. Résolu par un template release-gate qui signe et date l’exécution au tag.

RÉFÉRENCE	EXIGENCE	STATUT	CRITICITÉ	PREUVE / ÉCART
Annexe IV §1(h)	Procédures de validation, mesures par sous-groupe démographique	◐ Partial	HIGH	Mesures par sous-groupes calculées dans le pipeline d'entraînement (fairlearn) mais non exportées par système livré. Remédiation matérielle : construire un job d'export qui produit les tables par sous-groupes par système à chaque release.
Annexe IV §2(b)	Choix de conception, hypothèses et justifications	× Missing	HIGH	Aucune model card ni journal de décisions de conception pour les trois systèmes. Travail neuf : une model card par système, environ une journée de rédaction par système à partir de la mémoire d'ingénierie existante.
Annexe IV §2(g)	Journaux de tests validant la performance sur des entrées représentatives	◐ Partial	MEDIUM	Journaux de tests présents dans W&B ; non signés et datés comme l'exige l'Annexe IV. Même correctif release-gate que §1(g).

RÉFÉRENCE	EXIGENCE	STATUT	CRITICITÉ	PREUVE / ÉCART
Annexe IV §9 / Art. 72	Plan de surveillance après commercialisation	× Missing	CRITICAL	Aucun plan de surveillance après commercialisation. Surveillance de dérive ad-hoc et non connectée aux mesures par sous-groupes. Plus gros chantier neuf de la mission.
Article 73	Workflow de notification d'incidents graves (horloges 15 / 10 / 2 jours)	◐ Partial	HIGH	Astreinte et processus d'incident en place ; aucun SLA détection-vers-notification défini pour les incidents qualifiés règlement IA. Huit heures de design de processus comblent l'écart.

STATUS

✓ Satisfait — l'artefact existant satisfait l'exigence.

◐ Partiel — l'artefact existe ; sa forme, sa signature ou sa portée manque l'exigence.

× Manquant — aucun artefact aujourd'hui ; production neuve nécessaire.

SEVERITY

CRITICAL Critique — bloque le dossier technique ; à remédier en priorité.

HIGH Élevée — écart matériel ; à remédier dans la fenêtre du Sprint.

MEDIUM Moyenne — refermable en moins de quatre heures de travail.

LOW Faible — cosmétique ; à clore à la prochaine release.

SECTION 4

Registre des risques Article 9 — amorce

Le système de gestion des risques Article 9 est un processus documenté, sur tout le cycle de vie. Les cinq lignes ci-dessous sont les risques amorces identifiés pendant le Diagnostic ; le registre complet est construit pendant le Sprint et maintenu dans le cadre de la mission.

RISQUE	PROBABILITÉ	CRITICITÉ	MESURE D'ATTÉNUATION
Dérive de performance par sous-groupe sur le matcher après mise en production	MEDIUM	HIGH	Revue trimestrielle des mesures par sous-groupes ; seuils d'alerte câblés sur l'astreinte.
Signaux CV hallucinés par le LLM de tri (employeurs fabriqués, dates mal extraites)	LOW	MEDIUM	Validation de schéma de sortie ; vérification de cohérence par LLM-judge sur un échantillon glissant à 1 % ; affordance UI de spot-check par les recruteurs.
Amplification de biais à travers le pipeline matcher → screener → scoring d'entretien	MEDIUM	HIGH	Tests par tranche à chaque étape ; surveillance consciente du couplage ; évaluation d'équité bout-en-bout trimestrielle sur cohorte tenue à part.
Détournement des sorties pour des décisions d'embauche hors du périmètre documenté	LOW	HIGH	Clause contractuelle de périmètre dans les CGV client ; affordances UI ; attestation de conformité côté client trimestrielle.
Dérive de données après intégration d'un nouvel ATS chez un client	MEDIUM	MEDIUM	Set d'évaluation glissant par client ; cadence de réentraînement définie ; gate d'onboarding par client.

SECTION 5

Plan de surveillance après commercialisation Article 72 — esquisse

Le plan de surveillance après commercialisation est le plus gros chantier documentaire neuf. Esquisse ci-dessous ; plan complet livré comme artefact du Sprint.

TÉLÉMÉTRIE COLLECTÉE PAR INFÉRENCE	Snapshot de distribution d'entrée (caractéristiques catégorielles et numériques) ; confiance de prédiction ; action en aval observée (clic, contact, demande d'entretien, embauche) ; identifiant client et version du système.
SUIVI PAR SOUS-GROUPES	Par système, tous les 30 jours, par attribut protégé (lorsque la donnée est disponible et licite à suivre). Résultats écrits dans un dashboard versionné de mesures par sous-groupes et exportés vers l'annexe du dossier technique à la revue trimestrielle.
SEUILS DE DÉRIVE	Seuil de glissement de population : dix pour cent de divergence KL sur la distribution des caractéristiques d'entrée déclenche une revue. Seuil d'écart de performance par sous-groupe : cinq pour cent absolu sur tout sous-groupe suivi déclenche escalade.
CADENCE DE REPORTING	Revue interne mensuelle par le lead ingénierie. Rapport écrit trimestriel co-signé par le lead ingénierie et le Partner. Revue externe annuelle (optionnelle, recommandée au format Programme).
LIAISON AVEC L'ARTICLE 73	Tout événement détecté par la surveillance après commercialisation qui satisfait la définition d'incident grave de l'Article 3(49) déclenche la procédure d'incident (Section 6) et démarre les horloges 15 / 10 / 2 jours.

SECTION 6

Procédure de notification d’incidents Article 73

L’Article 73 impose les horloges de notification 15 / 10 / 2 jours. La procédure convertit la détection d’astreinte en rapport prêt pour le régulateur.

CONDITIONS DE DÉCLENCHEMENT	Définition d’incident grave Article 3(49) opérationnalisée par rapport aux trois systèmes. Exemples : un résultat d’embauche matériellement altéré par une défaillance modèle ; une violation de performance par sous-groupe au-delà des mesures d’atténuation ; un incident de fuite de données exposant le contenu de CV.
SLA DE CLASSIFICATION	T+24 heures après détection par l’astreinte : un appel de classification ingénierie + Partner décide si l’événement est un incident grave Article 73.
HORLOGES DE NOTIFICATION	15 jours pour les incidents graves généraux ; 10 jours en cas de préjudice grave avéré ou probable ; 2 jours pour une infraction étendue au droit de l’Union. Templates pour chaque horloge inclus dans le livrable.
CHAÎNE D’ESCALADE	Ingénieur d’astreinte → lead ingénierie → Partner → conseil externe (si requis) → notification à l’autorité nationale compétente.

SECTION 7

Feuille de route de remédiation à 26 semaines

Calendrier jusqu'au 2 août 2026, date d'application des obligations à haut risque Annexe III. Les responsables affichés sont des intitulés de rôle indicatifs ; les responsables nommés sont arrêtés au kickoff du Sprint.

SEMAINES	CHANTIER	RESPONSABLE	LIVRABLE
1–4	Refermeture des écarts documentaires	Lead ingénierie + Partner	Trois model cards · journaux de validation signés (template release-gate) · journal de décisions de conception · document d'interaction §1(c).
5–10	Plan de surveillance après commercialisation opérationnel	Lead ingénierie	Plan PMM v1.0 · exports de mesures par sous-groupes par système · alarmes de dérive câblées sur l'astreinte · cadence de revue mensuelle en production.
11–16	Système de gestion des risques Article 9 documenté	Partner + Conformité	SGR documenté · registre des risques synchronisé avec les alarmes PMM · processus de revue trimestrielle.
17–22	Workflow de notification d'incidents Article 73	Lead astreinte + Partner	Règles de détection · SLA de classification câblés sur l'astreinte · templates de notification pour chacune des horloges 15 / 10 / 2 jours.
23–26	Dossier technique Annexe IV v1.0	Partner	Dossier technique Annexe IV unifié avec pages de signature · pack de hand-off · lettre d'évaluation de préparation pour usage achats.

SECTION 8

Étape suivante

TalentFit AI est dans le périmètre des obligations à haut risque sur les trois systèmes en production. Les artefacts déjà présents dans la stack d’ingénierie couvrent environ deux tiers de l’Annexe IV ; le tiers restant est concentré sur trois chantiers (surveillance après commercialisation, model cards, exports de mesures par sous-groupes) qu’un Sprint de deux semaines traite de bout en bout. Le chemin recommandé est un Sprint de mise en conformité démarrant sous dix jours ouvrés après acceptation, suivi de la feuille de route à 26 semaines ci-dessus.

Chiekh Alloul, Partner · Tenth Partner · 6 mai 2026