Maxime IFFLAND Baptiste Bischoff

Cahier des charges

Solution de gestion des conflits interne et harcèlement

Maxime IFFLAND
03/12/2025

1. PRÉSENTATION DU PROJET

1.1 Identité du projet

Désignation	Information	Source(s)
Nom du projet	Gestion de conflits internes en entreprise (LegalTech)	Doc 01, 09
Maîtrise d'Ouvrage (MOA / Client)	**HRComplianceTech Solutions** (PME LegalTech)	Doc 02, 03
Représentant MOA	Mme Caroline Morel, Responsable Produits Conformité	Doc 03, 04
Maîtrise d'Œuvre (MOE / Prestataire)	**Maxime IFFLAND et Baptiste BISCHOFF** (Équipe de développement)	
Période du projet	De Novembre 2025 à Avril 2026	Doc 03, 04
Date de rédaction du CdC	**03/12/2025**	

1.2 Documents de référence

Type de Document	Référence	Enjeu Principal
Cadre Législatif 1	Loi n° 2016-1691 du 9 décembre 2016 (dite **Loi Sapin 2**)	Obligation de dispositif d'alerte, garantie de l'anonymat et confidentialité.
Cadre Législatif 2	**Règlement Général sur la Protection des Données (RGPD)**	Sécurité des données (chiffrement), durée de conservation limitée.

Cadre Législatif 3	Code du travail	Gestion des cas de harcèlement, discrimination et d'atteintes éthiques.
Document Projet 1	Fiche Projet Détaillée (01)	Spécifications techniques et fonctionnelles initiales (Modules : Bureau, Webapp, API IA).
Document Projet 2	Entretien Client (04)	Précisions sur les besoins (Offline, journalisation inaltérable, choix MySQL).

2. CONTEXTE ET ENJEUX

Cette section a pour but de définir les raisons profondes (le contexte), les motivations (les objectifs) et les acteurs clés (les parties prenantes) du projet.

2.1 Contexte et Problématique Actuelle

Le projet s'inscrit dans un contexte réglementaire fort, principalement régi par la **Loi Sapin 2** (encadrant le dispositif d'alerte éthique) et le **RGPD** (encadrant la gestion des données personnelles sensibles).

Présentation du Client : HRComplianceTech Solutions

HRComplianceTech Solutions est une PME de 70 salariés, spécialisée dans l'édition de logiciels pour les Directions des Ressources Humaines (DRH) et les fonctions de conformité (*LegalTech*).

Problématique Actuelle et Enjeux Critiques

Face à l'obligation légale des entreprises (notamment PME et ETI) de mettre en place un dispositif de recueil de signalements, le client constate que ses propres clients gèrent ces situations de manière **artisanale** (emails, formulaires papier). Cette approche présente des **risques majeurs** (selon le Doc 03 et l'entretien client), qui sont les enjeux critiques du projet :

1. **Risque de Non-Conformité et Sanctions** : L'absence d'outil dédié entraîne un manque de **traçabilité**, une difficulté à garantir la **sécurité et la confidentialité** des données (chiffrement). Ceci expose l'entreprise cliente à des sanctions de l'Autorité des Marchés Financiers (AMF), de l'Agence Française Anticorruption (AFA) ou de la CNIL.
2. **Risque Réputationnel et Climat Social** : Une mauvaise gestion ou une fuite d'information peut engendrer une **détérioration du climat social** interne, une perte de confiance des salariés et une atteinte grave à la **réputation** de l'entreprise.

Le projet vise donc à fournir à HRComplianceTech Solutions un produit commercialisable qui apporte une réponse technique et légale structurée à ces deux risques.

2.2 Objectifs du Projet

L'objectif principal du projet est de développer une solution logicielle complète, modulaire et sécurisée pour la gestion des signalements internes.

Objectif Commercial

L'objectif est la **livraison d'un produit complet, fonctionnel et terminé** qui soit immédiatement intégré à l'offre de HRComplianceTech Solutions et puisse être commercialisé auprès de ses clients.

Objectifs Fonctionnels et Techniques

Type d'Objectif	Description	Référence(s)
Modularité	Concevoir une solution en trois modules distincts mais communicants : une **Application Bureautique (offline)**, une **Webapp d'administration**, et une **API sécurisée**.	Doc 01, 03
Conformité Légale	Garantir la stricte application de la Loi Sapin 2 et du RGPD, notamment le **respect de l'anonymat**, la **confidentialité** et la **journalisation inaltérable** des étapes de traitement.	Doc 04, 05
Automatisation	Intégrer un module d'**Intelligence Artificielle** (LLM) pour la classification automatique des signalements (harcèlement, corruption, éthique, etc.) et l'aide à la réponse initiale.	Doc 01, 04
Sécurité	Assurer le **chiffrement fort** des données sensibles et des pièces jointes, tant en transit qu'au repos (en base de données).	Doc 03, 04

2.3 Périmètre et Parties Prenantes

Le périmètre du projet inclut la conception de l'architecture logicielle, le développement des trois modules (Client lourd, Web, API IA), la sécurisation de la base de données, ainsi que la production des documentations nécessaires.

Partie Prenante	Rôle dans le Projet	Intérêts / Exigences
Maîtrise d'Ouvrage (MOA)	HRComplianceTech Solutions (Mme Morel)	Validation des fonctionnalités, respect du calendrier, qualité commerciale du produit final.
Maîtrise d'Œuvre (MOE)	Maxime IFFLAND et Baptiste BISCHOFF	Développement technique, architecture, gestion de projet (rédaction du CdC).
Utilisateurs Finaux 1 (Déposants)	Salariés de l'entreprise cliente	Dépôt facile et sécurisé (offline), garantie de l'anonymat et du suivi confidentiel.
Utilisateurs Finaux 2 (Gestionnaires)	Services RH et Juristes de l'entreprise cliente	Tableau de bord de suivi, classification automatique (IA), messagerie anonyme.
Partenaires Techniques (DSI/IT)	Service Informatique du client final	Installation et maintenance de l'application bureautique (Windev) et de l'infrastructure API/BDD.
Partenaires Métier (Consultants)	Formateurs et Consultants HRComplianceTech	Rédaction du contenu de formation des utilisateurs et sensibilisation au harcèlement (aide à l'intégration du produit chez les clients).

Contrainte Géographique : Hébergement

L'hébergement des données et de l'API devra être effectué sur des serveurs garantissant la **souveraineté des données**, c'est-à-dire situés en **France ou en Europe**, excluant tout cloud soumis aux législations extra-européennes (ex: Cloud Act américain).

3. BESOINS FONCTIONNELS

Cette section décrit les fonctionnalités attendues par l'utilisateur final et les gestionnaires pour chacun des trois modules.

3.1 Module 1 : Application Web de Dépôt (Web - Utilisateur Salarié)

Ce module, développé en **Next.js/React** , est le point d'entrée du signalement et doit privilégier la simplicité d'usage et la sécurité maximale de l'anonymat. Il est accessible via un navigateur

ID	Exigence Fonctionnelle	Description Détaillée
F.1.1	Formulaire de Signalement Guidé	L'application Web doit présenter un formulaire clair et intuitif permettant de renseigner : la catégorie du signalement (Harcèlement, Fraude, Discrimination, Éthique, Autre), la description détaillée des faits, la date, le lieu, et les personnes impliquées (si connues)[6].
F.1.2	Gestion des Pièces Jointes	Possibilité d'ajouter des preuves (max. 3 pièces jointes) aux formats usuels (PDF, JPG, PNG, Audio). Le système doit chiffrer ces fichiers avant l'envoi à l'API[7].
F.1.3	Choix du Mode de Dépôt	L'utilisateur doit choisir entre : **Signalement Anonyme** (aucune donnée d'identification n'est demandée) ou **Signalement Confidentiel** (l'identité est transmise aux gestionnaires habilités uniquement)[8].
F.1.4	Génération Code de Suivi	À la validation du signalement, un **code alphanumérique unique et non-identifiant** doit être généré et affiché au salarié. Ainsi qu'un **code de type mot de passe**. Ces codes sont les seules clés pour le suivi. La clé de type mot de passe permet de sécuriser le code alphanumérique qui peut être brut force[9].
F.1.5	Régime du Code Perdu (Sécurité Forte)	(Décision stratégique) Par priorité donnée à la sécurité et à l'anonymat (Loi Sapin 2), il ne doit exister **aucune procédure de récupération** du Code de suivi. En cas de perte, l'accès au suivi et à la messagerie est définitivement perdu, garantissant ainsi l'intégrité de l'anonymat du déposant[10].

Point de flou dans le projet F1.5 est encore à définir. Car il y a différentes possibilités, l'option la plus sécurisée est celle présentée dans le tableau. Mais les alternatives

peuvent être la réponse à des questions personnelles, ou un espace de suivi des signalements fait par l'utilisateur après une connexion.

3.2 Module 2 : Application de Gestion (Client Lourd/Windev - RH / Juristes)

Ce module est l'interface d'administration et de traitement des cas, développé en **Windev**. C'est une application bureautique installée sur les postes des Gestionnaires (RH / Juristes).

ID	Exigence Fonctionnelle	Description Détaillée
F.2.1	**Authentification et Gestion des Rôles**	Connexion sécurisée avec gestion des droits d'accès. Les rôles (Administrateur, Juriste, RH) doivent restreindre la visibilité des données sensibles (ex: les Juristes peuvent avoir accès à des informations que les RH n'ont pas)[17].
F.2.2	**Tableau de Bord et Filtrage**	Affichage de l'ensemble des signalements via un tableau de bord. Filtres obligatoires : Statut (Nouveau, En Cours, Clôturé), Catégorie, Date de dépôt, Mode (Anonyme/Confidentiel)[18].
F.2.3	**Traitement des Alertes**	Vue détaillée de chaque signalement. Fonctionnalités de : consultation des faits et des pièces jointes déchiffrées, ajout de notes internes (privées). Le Gestionnaire RH/Juriste doit pouvoir **corriger manuellement la catégorie proposée par l'IA**. L'historique (Audit Log) doit tracer à la fois l'affectation automatique initiale et la correction manuelle ultérieure, car la responsabilité finale de la qualification juridique du cas est humaine[19].
F.2.4	**Messagerie Anonyme**	Un outil de chat intégré permettant au Gestionnaire de communiquer de manière

		sécurisée et bidirectionnelle avec le déposant, sans que le Gestionnaire ne puisse identifier le déposant (uniquement via le Code de suivi)[20].
F.2.5	**Fonction d'Archivage/Anonymisation**	Une fois le traitement terminé, l'alerte doit pouvoir être clôturée et archivée. L'Administrateur doit avoir la possibilité de procéder à l'anonymisation irréversible des données personnelles conformément au RGPD[21].
F.2.6	**Journalisation d'Audit Inaltérable (Crucial Sapin 2)**	Un journal (audit log) doit enregistrer de manière horodatée, chiffrée et inaltérable (non modifiable) les actions suivantes : l'accès au dossier, le changement de statut, l'envoi d'un message, la consultation/téléchargement d'une pièce jointe, la clôture du dossier et l'anonymisation des données[22].
F.2.7	**Mode Offline (Capacité Windev)**	**L'application bureautique (Windev) doit permettre la consultation, l'ajout de notes internes, et la gestion du statut des signalements même en l'absence de connexion internet.** L'envoi et la mise à jour des données à l'API (synchronisation) doit être effectué automatiquement dès la reconnexion détectée.

3.3 Module 3 : API & IA

L'API est la couche métier sécurisée qui orchestre les échanges et les traitements automatisés.

ID	Exigence Fonctionnelle	Description Détaillée

F.3.1	API REST Sécurisée	Développer une interface RESTful (Python/Flask) qui gère l'authentification des requêtes et sert de passerelle unique entre les clients (Windev/Webapp) et la base de données.
F.3.2	Gestion du Chiffrement	L'API est responsable du chiffrement des données sensibles (description des faits, pièces jointes) dès leur réception et avant leur stockage en base.
F.3.3	Classification Automatique (Affectation)	(Décision stratégique) Dès la réception d'un signalement, l'API doit exécuter le module d'analyse textuelle (IA). Ce module doit **affecter automatiquement** la catégorie la plus probable au signalement. Cette affectation initiale (Automatique : [Catégorie]) doit être journalisée (F.2.6).
F.3.4	Génération de Réponses Standardisées	L'API doit pouvoir générer des messages prédéfinis (ex: accusé de réception) basés sur la catégorie détectée par l'IA ou définie par le gestionnaire.

4. BESOINS NON FONCTIONNELS

Les besoins non fonctionnels définissent les contraintes d'exécution et les qualités attendues du système, souvent liées à la sécurité, à la performance ou au cadre réglementaire.

4.1 Sécurité & Confidentialité (Critique)

La sécurité et la confidentialité sont les exigences non fonctionnelles les plus critiques pour ce projet (conformité Loi Sapin 2 et RGPD).

ID	Exigence	Description Détaillée
NF.4.1.1	**Chiffrement de Niveau Industriel**	Toutes les **données sensibles** (descriptions de faits, pièces jointes) doivent être chiffrées : **Au repos** (en base de données) via l'algorithme **AES-256 avec salage** (garantie maximale contre le déchiffrement non autorisé). **En transit** (entre les modules et l'API) via le protocole **HTTPS/TLS 1.2 minimum**. La **clé de chiffrement** sera stocké dans une variable d'environnement et ne doit être stockée ni dans la Base de Données ni dans le code source.
NF.4.1.2	**Journalisation Inaltérable (Audit Log)**	Toutes les actions des Gestionnaires (RH/Juristes) sur un dossier doivent être enregistrées dans un journal d'audit sécurisé et horodaté (cf. F.2.6). Ce journal doit être techniquement **inaltérable** pour servir de preuve légale en cas d'audit.
NF.4.1.3	**Authentification Renforcée (Application Windev de gestion)**	L'accès à la Application Windev de gestion (RH/Juristes) doit impérativement utiliser la **double authentification (MFA)** afin d'empêcher les accès illégitimes aux données sensibles (Décision stratégique)
NF.4.1.4	**Gestion des Sessions Sécurisées**	Une politique de sécurité des sessions doit être appliquée : déconnexion automatique de l'utilisateur après **15 minutes d'inactivité** sur l'application bureautique de gestion (RH/Juristes).

NF.4.1.5	**Anonymisation Irréversible**	La fonctionnalité d'archivage des dossiers clos doit permettre une **anonymisation irréversible et technique** des données personnelles du déposant (y compris les métadonnées et identifiants potentiels) conformément au droit à l'oubli.
NF.4.1.6	**Contrôle d'Accès basé sur les Rôles (RBAC)**	Le système doit garantir que seuls les utilisateurs explicitement désignés (RH, Juriste) et ayant la bonne habilitation peuvent accéder à un dossier, assurant la **confidentialité** des informations (Doc 05).
NF.4.1.7	**Mécanisme de Sauvegarde (RPO)**	Le système doit inclure un mécanisme de sauvegarde complète de la base de données (incluant les données chiffrées). La fréquence de sauvegarde minimale requise est fixée à **une fois par 24 heures (RPO de 24h)**. Les fichiers de sauvegarde doivent être stockés sur le serveur d'hébergement, dans un répertoire logiquement séparé de la base de données de production.
NF.4.1.8	**Alignement sur la norme ISO 27001**	La conception, le développement et la documentation du Système d'Information des Signalements devront être **alignés sur les principes de la norme ISO/CEI 27001** (Système de Management de la Sécurité de l'Information - SMSI), en particulier pour la gestion des risques, des accès, et la continuité de service.

4.3 Ergonomie & Performance

Malgré le faible volume de signalements, l'application doit offrir une expérience utilisateur professionnelle et optimisée, reflétant la qualité d'un éditeur de logiciel.

ID	Exigence	Description Détaillée
NF.4.3.1	**Optimisation de**	La Webapp et l'Application Bureautique doivent être conçues pour être fluides et réactives. Le temps de

	l'Expérience Utilisateur	réponse (chargement du tableau de bord, affichage du détail du cas) doit être **optimisé au maximum** pour garantir une excellente réactivité perçue par les Gestionnaires.
NF.4.3.2	**Accessibilité (Responsive Design)**	La Webapp de gestion (Module 1) doit être consultable et pleinement fonctionnelle sur différents supports (PC, Tablette) via un design **Responsif** (Doc 03).
NF.4.3.3	**Simplicité du Dépôt**	L'interface de dépôt (Module 2) doit être extrêmement simple et intuitive pour **encourager la libération de la parole** et minimiser le risque d'erreurs de saisie par le salarié (Doc 02).
NF.4.3.4	**Maintenance**	Le code doit être documenté, commenté, et versionné (GitHub) pour faciliter la maintenance corrective et évolutive par les équipes futures du client (Doc 03).

5. SPÉCIFICATIONS TECHNIQUES

Cette section détaille les choix technologiques et les exigences d'infrastructure arrêtés pour le projet.

5.1 Architecture Logicielle

L'architecture retenue est une architecture classique à **trois tiers (3-Tier Architecture)**, pour garantir la séparation des préoccupations, la scalabilité et la sécurité.

- **Tiers 1 (Présentation/Client)** : Il est composé de la **Webapp (Next.js) pour le Dépôt (Module 1)** et du **Client Lourd (Windev) pour la Gestion (Module 2)**.
- **Tiers 2 – Logique Métier et API (Python/Flask) : Ce Tiers est l'unique couche d'accès aux données (DB Layer)**. Il gère l'authentification, le chiffrement/déchiffrement et expose les données via des endpoints REST. L'accès direct au Tiers 3 est strictement interdit aux clients. **L'ORM SQLAlchemy est intégré au Module 3.**
- **Tiers 3 (Données)** : La base de données (PostgreSQL) et le système de stockage des fichiers chiffrés.

5.2 Stack Technique (Choix Arrêtés et Cibles)

Le choix des technologies est arrêté et non négociable.

Composant / Rôle	Technologie	Objectif et Rationale (Adapté à la nouvelle contrainte)
Frontend Webapp	**React / TypeScript**	Interface de Dépôt (Module 1). Utilisation de **React** pour la robustesse et **TypeScript** pour la sécurité du typage. Garantit le Responsive Design.
Requêtes HTTP	**Axios**	Client HTTP privilégié pour la gestion des Intercepteurs (injection du token d'authentification) et la gestion des erreurs API.

Validation JS	**Zod**	Assurer la validation des schémas de données et des formulaires côté client (Module 1) avec une bibliothèque simple, typée et performante.
Application de Gestion	**Windev** (Client Lourd)	Interface de Gestion (Module 2). Utilisation du client lourd pour garantir l'accès **hors ligne (Offline)** et la compatibilité avec l'environnement Windows (C.8.3.2).
API & Backend	**Python (Flask)**	Fournir une **API REST unique, performante et sécurisée**. Le choix de Python est privilégié pour l'intégration optimisée des librairies de sécurité, de chiffrement et d'IA/NLP.
DB Layer (ORM)	**SQLAlchemy**	**Désigné comme le DB Layer unique et intégré.** Cet ORM est utilisé **exclusivement par l'API Python/Flask**, garantissant qu'aucune autre application (ni Prisma) n'accède directement à la Base de Données (Tiers 3), renforçant ainsi la sécurité.
Base de Données	**MySQL**	Base de données Open Source, robuste et reconnue pour sa fiabilité (Hébergement Aiven.io).
Base de Données (IA)	**Vectoriel (ex: PGvector)**	Stockage des *embeddings* pour les traitements de Similarité et la Classification Automatique (F.3.3).
IA/NLP	**Librairies Open Source (ex: Scikit-learn, spaCy)**	Développer un modèle de classification adapté aux catégories juridiques spécifiques du projet.
Chiffrement	**`cryptography` et `bcrypt`**	Implémentation du chiffrement **AES-256** (`cryptography`) pour les données sensibles et du hachage des mots de passe (`bcrypt`).

5.3 Environnement (DevOps) et Hébergement

Cette section spécifie les outils de travail collaboratifs (DevOps) et les exigences d'infrastructure.

Outil	Usage	Rationale
IDE	**Visual Studio Code (VS Code)**	IDE de référence pour les technologies JavaScript/Python/BDD, favorisant l'efficacité et la collaboration.
Versionnement	**GitHub** (Dépôt privé)	Gestion du code source, suivi des versions et facilitation de la collaboration au sein de la MOE.
Gestion de Projet	**Notion**	Suivi des tâches, des sprints, documentation interne et gestion des exigences fonctionnelles.
Communication	**Discord**	Communication synchrone rapide au sein de l'équipe de développement.
Conteneurisation	**Docker**	Les environnements de développement et de test seront standardisés via des conteneurs. Ceci garantit que l'application (API, BDD) fonctionne de manière identique avant le déploiement final (évite les problèmes de *« ça marche sur ma machine »*).

Exigences d'Hébergement

- **Souveraineté des Données :** L'infrastructure de production finale (serveur de l'API et BDD) devra être physiquement localisée en **Europe (France)** afin de garantir la souveraineté des données et d'exclure l'application des lois extra-européennes (ex: Cloud Act).
- **Infrastructure :** Le déploiement s'effectuera sur un serveur dédié ou un VPS européen. Le client final (PME/ETI) sera responsable de l'installation du Client Lourd (Windev) sur les postes des déposants.

6. ORGANISATION ET LIVRABLES

Cette section établit le cadre de travail, le calendrier, les modalités de suivi et définit les livrables concrets qui seront remis à la Maîtrise d'Ouvrage (HRComplianceTech Solutions) en fin de projet.

6.1 Méthodologie et Suivi de Projet

Le projet sera conduit selon une approche **Agile Scrum**, afin de favoriser la flexibilité, la réactivité aux retours clients et la livraison progressive de valeur.

Méthodologie de travail

- **Cycles de Développement (Sprints) :** La durée standard d'un Sprint est fixée à **deux semaines (Bimensuel)**. Chaque Sprint doit aboutir à la livraison d'un incrément potentiellement livrable ou à la validation d'un ensemble de fonctionnalités.
- **Outils de Suivi :** La gestion des tâches (Backlog, Sprints) sera assurée via **Notion** (cf. 5.3) et la communication via **Discord**.
- **Suivi Hebdomadaire (Point client) :** Un point de suivi formel sera organisé **une fois par semaine** (Visio ou Mail, selon la disponibilité de Mme Morel) pour une durée maximale de 30 minutes (Doc 04).

Mesure de l'Avancement

Le suivi de projet visera à garantir la transparence de l'avancement. Lors des points hebdomadaires, le rapport inclura obligatoirement :

- **Rapport d'avancement (Burndown Chart) :** Un graphique d'avancement sera présenté pour visualiser le travail restant (en jours/points) par rapport au temps restant avant les jalons critiques (Démo intermédiaire et Livraison finale). (Décision stratégique)
- **Synthèse du Sprint :** Bilan des fonctionnalités terminées dans le Sprint écoulé et revue du Backlog pour le Sprint suivant.

Jalons Clés

Jalon	Date Cible	Objectif de la Livraison

Lancement du projet	Novembre 2025	Démarrage du développement, initialisation de l'environnement Docker, création du dépôt GitHub.
Validation du CdC	Semaine suivant la réception	Validation formelle des exigences entre MOA et MOE.
Démo Intermédiaire	Mi-Février 2026 (6e semaine de développement)	Démonstration d'une première version fonctionnelle : dépôt d'un signalement via Windev, passage par l'API (chiffrement/déchiffrement) et affichage du cas dans la Webapp de gestion (Doc 04).
Soutenance & Livraison Finale	Début Avril 2026	Remise de l'ensemble des livrables et soutenance du projet.

6.2 Liste des Livrables

Les éléments suivants seront remis au client HRComplianceTech Solutions à la date de livraison finale (Avril 2026).

Catégorie	Livrable	Description	Format
Logiciel	**Code Source**	Intégralité du code source des trois modules (API Python/Flask, Webapp Next.js, Client Lourd Windev).	Dépôt privé **GitHub** (accès à transférer au client).
Logiciel	**Exécutables et Déploiement**	Fichiers d'installation de l'application bureautique (Windev) et Webapp déployable (Conteneurs Docker pour API et Webapp).	Fichiers exécutables et images Docker.

Documentation	**Manuel Utilisateur**	Guide complet à destination des Salariés (dépôt) et des Gestionnaires (RH/Juristes) décrivant l'usage de la solution.	Document **PDF** (Décision stratégique).
Documentation	**Documentation Technique**	Documentation de l'API (endpoints), guide d'installation (serveur, BDD MySQL, conteneurs Docker) et description de l'architecture.	Fichiers (Markdown ou PDF).
Conformité	**Dossier de Conformité**	Document justifiant la conformité du dispositif à la **Loi Sapin 2** et au **RGPD** (y compris la gestion du chiffrement, de l'audit log et des durées de conservation).	Document PDF.
Données	**Jeu de Données Initial**	Script ou base de données avec un jeu de données d'entraînement pour le module IA.	SQL ou CSV.
Logiciel	**Fichiers de conteneurisation**	Fichier **Dockerfile, docker-compose.yml** pour le de l'API et de la Webapp en production	Dockerfile, docker-compose.yml

7. CRITÈRES DE VALIDATION (RECETTE)

La recette est la phase formelle par laquelle la Maîtrise d'Ouvrage (HRComplianceTech Solutions) valide la conformité du logiciel aux exigences définies dans ce Cahier des Charges (CdC). La validation sera effectuée lors de la Démonstration Intermédiaire (Mi-Février 2026) et de la Livraison Finale (Avril 2026).

7.1 Validation Fonctionnelle (Tests d'Usage)

L'application sera validée en exécutant des scénarios utilisateurs clés.

Critère de Validation	Scénario de Test	Exigence Correspondante
CV.7.1.1 (Cycle Anonyme)	Un signalement peut être déposé en mode **Anonyme** (Module 1 - WebApp. Le Gestionnaire (Module 2 - Windev) doit pouvoir **répondre** via la Messagerie Anonyme. Le déposant (Salarié) doit pouvoir **lire la réponse** en utilisant uniquement le Code de Suivi généré.	F.1.4, F.2.4
CV.7.1.2 (Anonymisation)	Un Gestionnaire doit pouvoir archiver et lancer la procédure d'anonymisation irréversible (F.2.5). Une vérification doit prouver que les données personnelles ont été effacées/masquées dans la base (MySQL).	F.2.5, NF.4.1.5
CV.7.1.3 (Rôles et Accès)	Un Administrateur doit pouvoir créer un compte Juriste et un compte RH. Chaque utilisateur ne doit voir que les dossiers pour lesquels il est habilité, et doit respecter la politique de déconnexion automatique (NF.4.1.4).	F.2.1, NF.4.1.4, NF.4.1.6
CV.7.1.4 (Offline)	Une alerte doit être saisie sur le Client Lourd (Windev) sans connexion réseau. L'alerte doit être stockée localement, puis	F.1.5

	synchronisée avec succès dès la reconnexion du poste à Internet.	

7.2 Validation Sécurité (Tests de Robustesse)

La validation de la sécurité est critique. Elle doit prouver que l'application respecte les exigences NF.4.1 (Chiffrement AES-256 et Audit Log inaltérable).

Critère de Validation	Méthode de Test	Exigence Correspondante
CV.7.2.1 (Chiffrement BDD)	**(Décision stratégique)** L'équipe MOE doit réaliser un test simulé : tenter d'accéder directement au serveur de base de données (MySQL), lire les champs sensibles, et prouver qu'ils sont **illisibles et non déchiffrables** sans la clé de chiffrement présente dans l'API.	NF.4.1.1
CV.7.2.2 (Journalisation Inaltérable)	Un changement de statut (Ex : Nouveau -> En cours) doit être effectué. L'équipe MOA vérifiera la présence de l'entrée correspondante dans le journal d'audit (Audit Log) et s'assurera qu'elle ne peut être ni modifiée ni supprimée via l'interface.	F.2.6, NF.4.1.2
CV.7.2.3 (Authentification MFA)	La connexion à l'application bureautique de gestion (Module 1) doit impérativement exiger une **Double Authentification (MFA)** pour tous les rôles de gestionnaires	NF.4.1.3

7.3 Validation IA et Juridique

Critère de Validation	Description	Exigence Correspondante

CV.7.3.1 (Classification IA)	Le module IA doit exécuter la classification automatique lors de chaque nouveau dépôt. La catégorie proposée doit être **affectée automatiquement** au dossier pour faciliter le tri initial (F.3.3). L'équipe MOA validera la présence et la pertinence de la catégorie initiale (même si elle peut être corrigée manuellement).	F.3.3
CV.7.3.2 (Validation Légale)	Le **Dossier de Conformité** (Livrable 6.2) détaillant l'application de la Loi Sapin 2 et du RGPD doit être examiné et **validé formellement** par la Maîtrise d'Ouvrage (Mme Morel) ou son représentant juridique.	NF.4.2.4

8. CONTRAINTES

Cette section liste les contraintes non négociables (délai, budget, techniques et légales) qui encadrent la réalisation du projet et qui doivent être prises en compte par la Maîtrise d'Œuvre.

8.1 Contraintes de Délai et de Périmètre (Scope)

ID	Type	Contrainte	Impact / Règle
C.8.1.1	**Délai Fixe**	La date de livraison finale (Avril 2026) est fixe et ne peut être repoussée.	**Priorité au Délai** : En cas de difficulté imprévue, le périmètre fonctionnel (*scope*) sera ajusté en accord avec la MOA (Mme Morel) pour garantir le respect de la date de livraison.
C.8.1.2	**Dépendance Windev**	Le développement du Module 2 (Application de gestion) est conditionné par la prise en main et la maîtrise de l'outil **Windev** par l'équipe MOE.	Un temps significatif doit être alloué à la formation et à la prise en main de cet IDE spécifique.

8.2 Contraintes de Ressources Humaines et de Maintenance

ID	Type	Contrainte	Impact / Règle
C.8.2.1	**Ressources Limitées**	L'équipe de développement (MOE) est limitée à deux personnes (Maxime IFFLAND et Baptiste BISCHOFF).	La charge de travail doit être gérée via les Sprints Agiles (6.1) pour éviter la surcharge.

C.8.2.2	**Support Post-Livraison**	**(Décision stratégique)** Le projet n'inclut **aucune maintenance corrective, évolutive ou support technique** après la livraison finale (Avril 2026).	Le client (HRComplianceTech Solutions) doit anticiper l'internalisation des compétences techniques (Python, Next.js, Windev) pour assurer la pérennité de la solution.

8.3 Contraintes Techniques et Légales

ID	Type	Contrainte	Impact / Règle
C.8.3.1	**Chiffrement Fort**	Obligation d'utiliser l'algorithme de chiffrement **AES-256 avec salage** pour les données sensibles, y compris les pièces jointes, pour satisfaire aux exigences NF.4.1.1.	Tout choix technique contraire sera rejeté lors de la validation sécurité (CV.7.2.1).
C.8.3.2	**Exigence OS Client Lourd**	Le Module 2 (Client Lourd Windev) est conçu pour fonctionner sur un environnement **Windows 10 Pro ou supérieur**.	L'application n'est pas garantie sur les systèmes d'exploitation antérieurs ou non-Windows (Linux, macOS, Mobile).
C.8.3.3	**Authentification Application Bureautique**	**(Décision stratégique)** Le projet ne prendra pas en charge l'intégration avec les annuaires d'entreprise externes (LDAP/Active Directory).	L'authentification des gestionnaires RH/Juristes (Application de bureau) sera gérée par l'application elle-même (comptes locaux sécurisés).

C.8.3.4	**Conformité Juridique**	Respect obligatoire de la Loi Sapin 2 (anonymat, traçabilité) et du RGPD (durée de conservation, droit à l'oubli).	La non-conformité à ces textes entraînera la non-validation du livrable final (CV.7.3.2).
C.8.3.5	**Contrainte de licences**	Le projet intègre des technologies soumises à licence (ex: **Windev**). Logicielles pour la distribution du produit final.	Il est de la responsabilité de la MOA (HRComplianceTech Solutions) de s'assurer de la validité et de la couverture de ses licences

8.4 Contraintes Opérationnelles et Limites de Garantie

ID	Type	Contrainte	Impact / Règle
C.8.4.1	**RTO & PRA**	Le périmètre de la MOE se limite à la fourniture des mécanismes de sauvegarde (NF.4.1.7) et de l'architecture.	La **MOA (HRComplianceTech Solutions)** est responsable de la définition et de la mise en œuvre opérationnelle du **Plan de Reprise d'Activité (PRA)** et du **Délai de Reprise d'Activité (RTO)** après la livraison. Le MOE ne garantit pas de délai de restauration de service en production.