Dictionnaire de Données et Règles d'Intégrité

1. Objectif de la Base de Données (BDD)

Objectif Principal

L'objectif fondamental de la BDD est de **stocker et de gérer de manière sécurisée et structurée** l'intégralité des données relatives au dispositif de recueil de signalements internes (gestion des conflits et harcèlement), en assurant la conformité avec le cadre légal français et européen.

Rôles Clés de la BDD

- **Garantir la Conformité Légale (Loi Sapin 2 & RGPD)** : La BDD doit permettre le respect strict de la Loi Sapin 2 (traçabilité inaltérable des actions, garantie de l'anonymat) et du RGPD (chiffrement des données sensibles, droit à l'oubli).
- **Supporter l'Architecture en Trois Tiers** : Elle constitue le **Tiers 3 (Données)** de l'architecture logicielle, agissant comme le référentiel unique des données pour l'API (Tiers 2) qui orchestre le chiffrement et les règles métier.
- **Stockage Sécurisé** : Elle doit héberger non seulement les données structurées, mais aussi les **pièces jointes chiffrées**, garantissant leur confidentialité tant au repos qu'en transit.
- **Base du Journal d'Audit Inaltérable** : Elle est le support du journal d'audit (`audit logs`), crucial pour la traçabilité légale, enregistrant de manière chiffrée et non modifiable les actions des gestionnaires.

2. Liste des Données et Dictionnaire de Données

La BDD s'articule autour d'un ensemble d'entités (tables) principales pour gérer les signalements, les utilisateurs de gestion, et les données de conformité.

Entités Centrales et Sensibles

Nom de la Table	Description	Données Sensibles / Règle Clé
signalements	Enregistrement principal de l'alerte.	Contient la description détaillée des faits (`description, encrypted`), les informations de contact de la victime/mise en cause (`victum contact encrypted`),

		et le code de suivi (`tracking code`). **Toutes ces données sont chiffrées (AES-256) au repos**.
pieces jointes	Référence et métadonnées des preuves ajoutées au signalement.	Contient le chemin d'accès chiffré (`encrypted path`) et le nom de fichier original chiffré (`original biename encrypted`). Les fichiers eux-mêmes sont chiffrés avant stockage.
messages	Historique des échanges bidirectionnels entre le déposant anonyme et le gestionnaire.	Le contenu est chiffré (`contenu encrypted`) et la communication est anonyme pour le déposant.
audit logs	Journal d'historisation des actions des gestionnaires.	Enregistre de manière horodatée et chiffrée (`detals encrypten` [16]) chaque étape de traitement (accès, changement de statut, etc.). Assure l'inaltérabilité via un chaînage de hachage (`previous Rash`, `current hash`).

Entités de Gestion et Référentiels

Nom de la Table	Description	Attributs Clés	Contexte
users	Comptes des gestionnaires RH/Juristes.	`Ide`, `name`, `password hash`.	Utilisé pour l'authentification et le MFA.
role / permission	Gestion des droits d'accès.	`id role`, `name role` (ex: Juriste, RH).	Permet l'application du Contrôle d'Accès basé sur les Rôles (RBAC).

categorie	Types de signalements.	`id categorie, name.`	Utilisé pour le filtrage et la classification automatique par l'IA.
statut	Étapes de traitement du signalement.	`id statut, name.`	(Nouveau, En Cours, Clôturé) – Utilisé pour le tableau de bord et la traçabilité.
priorite	Niveau d'urgence du signalement.	`id priorite, priorite.`	Permet de hiérarchiser les cas dans le tableau de bord.
classifications IA	Proposition initiale de catégorie par l'IA.	`signalement id, categorie propose id.`	Trace l'affectation automatique par l'IA (qui peut être corrigée manuellement par l'humain).

3. Liste des Règles d'Intégrité et de Sécurité

La sécurité et l'intégrité des données sont critiques (NF.4.1). Les règles ci-dessous sont tirées des exigences fonctionnelles et non fonctionnelles du CdC (Sections 3.2, 4.1, 8.3).

Règle	Exigence Correspondante	Description Détaillée
Chiffrement au Repos (Critique)	NF.4.1.1 / C.8.3.1	Utilisation obligatoire de l'algorithme **AES-256 avec salage** pour chiffrer toutes les données et pièces jointes sensibles stockées dans la BDD. La clé de chiffrement doit être stockée hors BDD (variable d'environnement).
Chiffrement en Transit	NF.4.1.1	L'échange de données entre les modules et l'API doit être sécurisé via le protocole **HTTPS/TLS 1.2 minimum**.

Journalisation Inaltérable (Sapin 2)	F.2.6 / NF.4.1.2	L'accès et la modification des dossiers par les gestionnaires doivent être enregistrés dans un **Audit Log** sécurisé, horodaté et techniquement **inaltérable** (probablement via hachage chaîné comme suggéré par le schéma).
Anonymisation Irréversible (RGPD)	F.2.5 / NF.4.1.5	Une procédure doit garantir l'effacement définitif et l'anonymisation technique et irréversible des données personnelles du déposant (droit à l'oubli) lors de la clôture et l'archivage du dossier.
Authentification Renforcée (MFA)	NF.4.1.3	L'accès à l'Application de Gestion (Windev) par les RH/Juristes doit être protégé par une **double authentification (MFA)**.
Sécurité du Code de Suivi	F.1.5	Par priorité à l'anonymat, **aucune procédure de récupération** du `tracking code` et de son mot de passe associé n'est autorisée, garantissant l'intégrité du dépôt anonyme (décision stratégique Sapin 2).

Règles d'Intégrité et de Gestion des Données

Règle	Exigence Correspondante	Description Détaillée
Contrôle d'Accès basé sur les Rôles (RBAC)	F.2.1 / NF.4.1.6	La visibilité et la modification des données doivent être strictement conditionnées par le rôle de l'utilisateur (Administrateur, Juriste, RH). Les Juristes peuvent avoir accès à des informations restreintes aux RH.
Politique de Session	NF.4.1.4	Déconnexion automatique de l'utilisateur après **15 minutes d'inactivité** sur

		l'application de gestion pour minimiser le risque d'accès non autorisé.
Objectif de Point de Récupération (RPO)	NF.4.1.7	Une sauvegarde complète de la BDD (incluant les données chiffrées) est requise au minimum **une fois par 24 heures**.
Intégrité de la Classification IA	F.2.3	L'affectation de catégorie proposée par l'IA doit être journalisée, mais le gestionnaire (humain) doit pouvoir la corriger manuellement. L'historique (Audit Log) doit tracer l'affectation automatique *et* la correction manuelle.