# Registre des Risques Liés aux Données

Entreprise : OptiValue.ai  
Version : 1.0  
Date : 03/09/2025  
Auteur : Délégué à la Protection des Données (DPO)

## Introduction

Le présent registre recense les risques liés aux données traitées par OptiValue.ai, conformément au RGPD, à l’ISO 27701, et aux standards ISO 31000. Il permet de piloter les risques par domaine, par niveau de criticité et par cycle de vie des données (collecte, traitement, conservation, suppression). Ce registre est mis à jour en continu via la plateforme ComplianceHub.ai et validé trimestriellement par le DPO et le Comité de Gouvernance des Données.

## 1. Gouvernance et Processus

• Supervision par le DPO et les Privacy Champions dans chaque département.  
• Mise à jour mensuelle automatisée avec vérification manuelle.  
• Audit interne trimestriel et audit externe annuel pour certification.  
• Reporting consolidé au Comité Exécutif et au Conseil d’Administration.

## 2. Tableau des Risques Liés aux Données

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Filière / Processus | Risque | Cause | Impact | Probabilité | Mesures de contrôle existantes | Niveau résiduel | Responsable | Plan d’action |
| DR-001 | Plateforme SaaS | Fuite de données clients critiques | Mauvaise configuration cloud | 5 | 2 | Chiffrement AES-256, MFA, audit mensuel | 2 | RSSI | Renforcer contrôle d’accès et tests pentest mensuels |
| DR-002 | Support client | Accès non autorisé aux tickets sensibles | Droits d’accès mal configurés | 4 | 3 | Revue trimestrielle des accès, segmentation réseau | 2 | Directeur Support | Mise à jour IAM et sensibilisation |
| DR-003 | R&D IA | Biais dans les modèles | Données d’entraînement non équilibrées | 4 | 3 | Audits trimestriels, comité éthique | 2 | Responsable IA | Retraining modèles avec datasets validés |
| DR-004 | Marketing | Usage abusif de données pour ciblage | Collecte non conforme | 3 | 2 | Opt-in strict, audit prestataires | 1 | CMO | Audit supplémentaire et contrôle manuel |
| DR-005 | RH | Conservation excessive des données RH | Absence de purge automatique | 3 | 3 | Politique de conservation, purge manuelle annuelle | 2 | DRH | Automatiser le processus de purge |
| DR-006 | Audit & Sécurité | Journalisation insuffisante des accès sensibles | Logs non centralisés | 4 | 2 | SIEM centralisé, revue hebdomadaire | 2 | RSSI | Améliorer corrélation et alertes IA |

## 3. Suivi et Reporting

• Tableaux de bord dynamiques générés automatiquement avec classification par criticité.  
• Suivi en temps réel des plans d’action et alertes prédictives sur les risques émergents.  
• Revue mensuelle des risques par les responsables métiers et validation en comité RGPD.  
• Rapports consolidés pour le comité exécutif et les auditeurs externes.

## 4. Automatisation et Intégration

• Intégration du registre avec la plateforme ComplianceHub.ai.  
• Détection automatique des écarts ou anomalies grâce à l’IA.  
• Mise à jour instantanée des niveaux de criticité en cas de changement d’environnement technique ou réglementaire.

## 5. Amélioration Continue

• Analyse trimestrielle des incidents et ajustement des mesures de contrôle.  
• Comparaison avec des benchmarks sectoriels.  
• Intégration des recommandations issues des audits internes et externes.  
• Mise à jour annuelle validée par le Comité de Gouvernance des Données.

## Annexes

• Modèle de matrice de criticité.  
• Schémas des flux de données critiques.  
• Rapports de corrélation issus de l’IA.  
• Historique des incidents liés aux données.  
• Documentation sur les politiques de purge et conservation.