# Data Protection Impact Assessment (DPIA) - Modèle

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

## Introduction

Le présent modèle de Data Protection Impact Assessment (DPIA) est utilisé par OptiValue.ai pour évaluer et documenter les risques liés aux traitements de données personnelles. Ce modèle répond aux exigences de l'article 35 du RGPD et intègre les meilleures pratiques de l'EDPB, de l'ISO 27701 et des audits sectoriels.

## 1. Informations Générales

• Référence du projet : [À renseigner]  
• Responsable de traitement : OptiValue.ai  
• Responsable métier : [Nom, fonction]  
• Date de début du traitement : [Date]  
• Équipe projet : [Noms et rôles des participants]

## 2. Description du Traitement

• Objectifs et finalités du traitement.  
• Catégories de données collectées (ex : données personnelles, sensibles, anonymisées).  
• Sources des données et méthodes de collecte.  
• Technologies utilisées (ex : IA, cloud, API tierces).  
• Localisation des données et transferts hors UE (si applicable).

## 3. Base Légale et Nécessité

• Base légale invoquée (consentement, contrat, obligation légale, intérêt légitime).  
• Justification de la proportionnalité et de la nécessité du traitement.  
• Évaluation de l'adéquation des finalités aux données traitées.

## 4. Analyse des Risques

Chaque risque est identifié, évalué et priorisé selon une matrice 5x5 :  
• \*\*Risque 1\*\* : Fuite de données sensibles  
 - Probabilité : 2/5  
 - Impact : 5/5  
 - Mesures de mitigation : chiffrement AES-256, MFA, segmentation réseau, SOC 24/7.  
  
• \*\*Risque 2\*\* : Usage biaisé des algorithmes IA  
 - Probabilité : 3/5  
 - Impact : 4/5  
 - Mesures : audits algorithmiques trimestriels, comité éthique, explicabilité renforcée.

## 5. Mesures de Sécurité et Contrôles

• Chiffrement systématique des données au repos et en transit.  
• Authentification forte pour tous les accès sensibles.  
• Surveillance 24/7 via SOC et IA prédictive.  
• Tests d’intrusion trimestriels et audits annuels ISO 27001.  
• Journalisation et traçabilité complète des accès et traitements.

## 6. Évaluation Résiduelle des Risques

Après mise en place des contrôles, les risques résiduels sont évalués et approuvés par le DPO et le Comité de Gouvernance. Une revue trimestrielle est réalisée pour ajuster les mesures si nécessaire.

## 7. Plan d’Action

• Actions immédiates à mettre en œuvre.  
• Plans correctifs avec responsables et échéances.  
• Suivi trimestriel des indicateurs clés (KPI/KRI).  
• Rapports d’avancement partagés avec les parties prenantes.

## 8. Validation et Signatures

• Responsable de traitement : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date : \_\_\_\_  
• Délégué à la Protection des Données : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date : \_\_\_\_  
• Comité Éthique : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date : \_\_\_\_

## Annexes

• Matrice de scoring des risques.  
• Schéma des flux de données.  
• Historique des DPIA pour des projets similaires.  
• Exemples de rapports d’audit externe.  
• Documentation technique des mesures de sécurité.