ANALYSE D’IMPACT RELATIVE À LA PROTECTION DES DONNÉES (AIPD)

*Ce document est constitué de deux parties : la première est l’AIPD à compléter par vos soins, la seconde est une aide succincte pour la réalisation de l’AIPD. Ce modèle d’AIPD se veut aussi complet que possible. Sentez-vous libre d’omettre des éléments à votre convenance, tant que vous respectez le contenu minimum imposé par la loi.*

Version : [1.0]

Date : [JJ/MM/AAAA]

Responsable du traitement : [Nom de l’organisation]

Traitement évalué : [Nom du traitement]

**VALIDATION DU DOCUMENT**

|  |  |  |  |
| --- | --- | --- | --- |
| Rôle  | Nom  | Date  | Signature |
| Représentant du responsable du traitement |  |  |  |
| Conseiller à la protection des données |  |  |  |
| Responsable sécurité |  |  |  |
| Autre(s) |  |  |  |

**HISTORIQUE DES MODIFICATIONS**

|  |  |  |  |
| --- | --- | --- | --- |
| Version  |  Date  |  Auteur  |  Nature des modifications |
| 1.0  |  |  | Version initiale |

# RÉSUMÉ EXÉCUTIF

## Contexte

[Brève description du contexte et des objectifs du traitement]

## Conclusion principale

[Synthèse de l’évaluation et décision sur l’acceptabilité des risques]

## Points d’attention majeurs

[Liste des principaux risques et mesures critiques]

# DESCRIPTION DU TRAITEMENT

## Identification du traitement

### Description générale

* Nom du traitement
* Description
* Finalités poursuivies

### Base juridique et intérêts poursuivis

* Base(s) légale(s) applicable(s)
* Intérêts poursuivis par l’organisation
* Justification de la légitimité

### Contexte organisationnel

* Position du traitement dans l'écosystème global de l'organisation
* Interactions avec d'autres traitements
* Dépendances fonctionnelles et techniques
* Impact business en cas d'arrêt du traitement

### Conformité réglementaire spécifique

* Réglementations sectorielles applicables
* Standards et normes à respecter
* Certifications pertinentes
* Codes de conduite applicables

## Périmètre du traitement

### Données traitées

|  |  |  |  |
| --- | --- | --- | --- |
| Catégorie de données | Description | Sensible (O/N) | Durée de conservation |
|  |  |  |  |

### Personnes concernées

|  |  |  |
| --- | --- | --- |
| Catégorie de personnes | Estimation du nombre | Vulnérabilité particulière |
|  |  |  |

### Destinataires

|  |  |  |  |
| --- | --- | --- | --- |
| Destinataire | Nature | Données concernées | Base légale du transfert |
|  |  |  |  |

### Flux de données

* Collecte
[Description des modalités]
* Communication interne
[Description des flux internes]
* Transferts à l’étranger
[Description des transferts avec la liste des pays impliqués et les garanties]

### Cycle de vie des données

* Modalités de création/collecte (si différent des flux de données)
* Processus d'archivage
* Procédures de suppression/anonymisation
* Gestion des backups
* Modalités de portabilité

## Moyens du traitement

### Description fonctionnelle

[Description détaillée du fonctionnement]

### Architecture technique

[Description de l’infrastructure et des outils/solutions]

### Mesures de sécurité existantes

* Mesures organisationnelles
* Mesures techniques
* Mesures juridiques

### Sous-traitants

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sous-traitant | Rôle | Garanties contractuelles | Localisation | Lieu de traitement des données |
|  |  |  |  |  |

# ÉVALUATION DE LA NÉCESSITÉ ET DE LA PROPORTIONNALITÉ

## Analyse de la nécessité

### Justification des données collectées

|  |  |  |
| --- | --- | --- |
| Catégorie de données | Nécessité | Alternative possible |
|  |  |  |

### Démonstration de la minimisation

[Explication des choix de minimisation]

## Analyse de la proportionnalité

### Balance des intérêts

* Avantages du traitement
* Impacts sur les droits
* Conclusion sur la balance des intérêts

### Justification des durées de conservation

[Explication des durées retenues]

## Droits des personnes concernées

### Modalités d'exercice des droits

* Processus de gestion des demandes
* Outils et interfaces disponibles
* Délais de traitement
* Vérification de l'identité

### Information des personnes

* Contenu des mentions d'information
* Modalités de communication
* Mise à jour des informations
* Cas particuliers (mineurs, personnes vulnérables)

# ANALYSE DES RISQUES

## Identification des risques

### Sources de menaces

|  |  |  |
| --- | --- | --- |
| Source | Description | Motivation/Cause |
|  |  |  |

### Scénarios de risques

|  |  |  |
| --- | --- | --- |
| ID | Scénario | Impact potentiel |
|  |  |  |

## Évaluation des risques

### Matrice des risques

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Risque | Gravité(1-4) | Probabilité(1-4) | Score | Mesures existantes | Risque résiduel |
|  |  |  |  |  |  |

### Détail des risques

[Description détaillée des impacts par risque]

### Cartographie des contrôles

* Contrôles préventifs
* Contrôles détectifs
* Contrôles correctifs
* Évaluation de l'efficacité des contrôles

## Mesures prises ou à prendre relativement aux risques

### Plan d’action

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mesure | Risque traité | Responsable | Échéance | Statut |
|  |  |  |  |  |

### Réévaluation des risques résiduels

[Analyse des risques après mesures]

# VALIDATION ET SUIVI

## Avis des parties prenantes

### Avis du conseiller à la protection des données

[Avis détaillé]

### Avis des représentants des personnes concernées

Par exemple, une représentation du personnel de l’entreprise sur le traitement soumis à AIPD concerne les données de collaboratrices et collaborateurs

[Synthèse des consultations]

### Avis de l’autorité de protection des données

Si aucun conseiller à la protection des données n’a été consulté (art. 23 al. 4 LPD)

[Synthèse des échanges]

## Décision et validation

### Décision sur l’acceptabilité

* Conclusion
* Justification
* Conditions éventuelles

### Plan de suivi

* Indicateurs de suivi
* Fréquence de réexamen
* Responsables du suivi

## Gestion des incidents

### Procédures de gestion des incidents

* Processus de détection
* Chaîne d'escalade
* Procédures de notification (autorités, personnes concernées)
* Retours d'expérience

### Plan de continuité/reprise

* Mesures de continuité d'activité
* Procédures de reprise
* Tests et exercices
* Maintenance du plan

# ANNEXES

Annexe 1 : Documentation technique

[Documents techniques pertinents]

Annexe 2 : Schémas et diagrammes

[Schémas des flux, architecture, etc.]

Annexe 3 : Documents complémentaires

[Autres documents pertinents]

Annexe 4 : Registre des versions et modifications

* Historique détaillé des modifications
* Justifications des changements
* Impact sur l'évaluation des risques

Annexe 5 : Méthodologie

* Critères d'évaluation utilisés
* Échelles de notation
* Sources de données utilisées
* Limites de l'analyse

Annexe 6 : Plan de formation et sensibilisation

* Programmes de formation
* Matériel de sensibilisation
* Planning des sessions
* Évaluation des connaissances

Aide pour la réalisation d’une AIPD

# Équipe minimale et ressources nécessaires

* Conseiller à la protection des données
* Responsable métier du traitement
* Expert sécurité/IT
* Expert juridique
* Représentants des personnes concernées (si pertinent)
* Documentation technique et fonctionnelle du traitement

# Exemples de risques pour les personnes concernées

|  |  |
| --- | --- |
| Atteinte à l’intégrité physique ou mentale | Atteinte à la dignité humaine |
| Atteinte à la liberté académique et scientifique | Atteinte à la liberté d’expression |
| Atteinte à la liberté de mouvement | Atteinte à la liberté de réunion et d’association |
| Atteinte à la réputation | Atteinte à la sécurité personnelle |
| Atteinte à la vie privée | Atteinte aux droits de l’enfant |
| Discrimination | Manipulation politique |
| Perte d’autonomie décisionnelle | Perte de contrôle sur ses données personnelles |
| Perte du droit à l’oubli | Préjudice économique |
| Usurpation d’identité | Violation de l’égalité des chances |
| Violation de la liberté de croyance et de religion | Violation du secret professionnel |

# Exemples de critères d’évaluation

## Échelle de gravité (impacts)

1. Négligeable : Pas d’impact sur les personnes

2. Limité : Gêne mineure, réversible facilement

3. Important : Conséquences significatives, difficiles à surmonter

4. Maximum : Conséquences irréversibles, mettant en danger les personnes

## Échelle de probabilité

1. Négligeable : Très improbable

2. Limitée : Possible mais rare

3. Importante : Significative dans les circonstances

4. Maximum : Quasi certaine

## Matrice de criticité des risques

Score de risque = Gravité x Probabilité

* 1-4 : Risque faible — Acceptable
* 5-9 : Risque modéré — À surveiller
* 10-12 : Risque élevé — Mesures nécessaires
* 13-16 : Risque critique — Mesures urgentes requises

# Conseils d’utilisation

## Adopter une approche proportionnée

* Adapter le niveau de détail à la criticité du traitement
* Se concentrer sur les risques significatifs
* Documenter les choix méthodologiques

## Impliquer les bonnes parties prenantes

* Constituer une équipe pluridisciplinaire
* Consulter les experts pertinents
* Valider avec les responsables appropriés

## Maintenir l’AIPD dans le temps

* Définir un calendrier de revue
* Mettre à jour en cas de changement significatif
* Conserver l’historique des évaluations

## Intégrer l’AIPD dans la gouvernance

* Lier aux autres processus (sécurité, conformité)
* Utiliser les résultats pour les décisions
* Suivre la mise en œuvre des plans d’action