# Politique de protection des données

## 1 Contexte

### 1.1 Introduction

Mon entreprise déploie des activités dans les domaines de [liste non exhaustive]

Elle est amenée à traiter des données personnelles et des données sensibles au sens de la loi fédérale sur la protection des données concernant principalement les catégories de personnes physiques suivantes : [liste non exhaustive]

Cette politique décrit les principes et règles générales à respecter dans le cadre du traitement des données personnelles et sensibles.

### 1.2 But de la politique

Cette politique doit permettre à mon entreprise d'atteindre les objectifs suivants :

1. Respecter le cadre légal,
2. Garantir la transparence sur les traitements mis en œuvre,
3. Assurer que les droits des personnes concernées sont protégés,
4. Être capable de répondre efficacement aux demandes d'exercice de droit des personnes concernées,
5. Réduire les risques tant pour les personnes concernées que pour mon entreprise,
6. Prévenir les violations de la sécurité des données.

### 1.3 Champ d'application

*Exclure ou inclure certaines activités spécifiques, ou sociétés si on est en présence d'un groupe de sociétés, ou certaines catégories de fonctions au sein de l'entreprise*

### 1.4 Droit applicable

Le droit général de la protection des données est applicable [LPD, RGPD, etc.]

*S'il existe des lois sectorielles imposant certaines obligations, les mentionner ici.*

## 2 Principes généraux

*Rappeler ici les principes de protection des données en les expliquant succinctement*

- Principe de responsabilité (documenter, même brièvement, ce qu'on fait, pourquoi, comment, les risques, etc.)
- Principe de finalité (ne pas traiter de données sans savoir précisément à quoi elles servent)
- Principe de licéité (déterminer la base juridique)
- Principe de proportionnalité (ne pas traiter plus de données que nécessaire, supprimer lorsqu'on n'en a plus besoin)
- Principe de la bonne foi (être honnête dans la mise en œuvre des traitements)
- Principe de transparence (informer correctement les personnes concernées)
- Principe de l'exactitude (conserver les données à jour)
- Principe de sécurité (traiter les données d'une manière sûre)

 

# 3 Risques

*Détailler ici les risques principaux pour les personnes concernées que l'entreprise doit éviter de matérialiser, par exemple*

- Divulgation de données personnelles à des tiers non autorisés
- Transfert de données personnelles sans garanties appropriées
- Atteinte aux intérêts matériels ou financiers des personnelles concernées

*Détailler ensuite ceux qui la concernent directement et qu'elle veut éviter de matérialiser, par exemple*

- Lacune dans les mesures de sécurité menant à un incident
- Dégât d'image

# 4 Rôles et responsabilités

*Rappeler de manière succincte quelles sont les grandes responsabilités des organes et des unités de l'entreprise, par exemple*

4.1 Conseil d'administration
4.2 Direction
4.3 DPD
4.4 Équipes métier
4.5 Équipes projet
4.6 Équipes informatiques
4.7 Équipes marketing et vente
4.8 Équipes RH

# 5 Règles générales

*L'entreprise peut indiquer ici des règles générales sur le traitement des données personnelles et, le cas échéant, quelques mesures relevant du principe « privacy by design », par exemple*

- Clear desk policy
- Armoires, tiroirs fermés à clé
- Consultation obligatoire du DPD au début de la phase de cadrage de chaque projet, en cas de modification d'un traitement, etc.
- Annonce obligatoire des incidents
- Formation obligatoire une fois par année
- Gestion des droits d'accès aux données respectant le « need-to-know »
- Règles spécifiques aux données sensibles

# 6 Dispositions finales

 