Modèle de rapport de recommandations RGPD

Titre du projet	*Régulation des données aux normes du RGPD*

Version	Auteur	Description	Date
V1	*Loïc Stéphane BAMENOU*	*Rapport synthèse des nouvelles obligations ou recommandations à mettre en œuvre par la société DEV'IMMEDIAT pour la continuité de ces opérations/activités face aux normes du RGPD*	*27.12.2023*

Introduction

Ce rapport synthèse de régulation des normes de traitements des données personnelles a vu le jour en raison des sanctions qui nous sont appliquées par la CNIL [1]sur le non-respect des règles du RGPD[2]. Ces sanctions proviennent de la revendication d'un assuré sur la conservation de ces données personnelles sur une période relativement longue sans son autorisation.

À la suite de cet événement, votre société a mandaté le consultant que je suis pour vous aider à intégrer les règles et normes du RGPD dans ses processus d'activité. À cet effet, nous avons établi, avec la collaboration des différents services de l'entreprise, un ensemble de règles à appliquer pour l'utilisation des données de sa clientèle. Ces nouvelles règles permettront ainsi la collecte, le traitement et l'exploitation des données de ces assuré(e)s sans craindre de nouvelles sanctions de la CNIL.

[1] CNIL : Commission Nationale de l'Informatique et des Libertés ;

[2] RGPD : Règlement général de Protection des données ;

DEV'IMMEDIAT

Contenu du rapport

I. Propositions de recommandation pour le respect des normes du RGPD

Dans cette nouvelle démarche d'incorporation les règles du RGPD dans votre processus d'activité, nous avons proposé sept (07) recommandations qui se structurent en deux grandes catégories à savoir :

- ***1ère Catégorie : Recommandations en lien avec des ressources humaines***
  - ✓ Mise en place d'un **service informatique de traitement de la donnée** sous la direction générale et en collaboration avec les différentes entités métiers. Ce service doit être composer d'une équipe Data Management Officer (interne ou externe à l'entreprise) :
    - Chief Data Officer (CDO)
    - Data Protection Officer (DPO)
    - Data Scientist/Business Analyst ;
  - ✓ Disposer de **référents dans les différents services pour remonter les besoins des métiers** à l'équipe Data Management Officer ;
- ***2ème Catégorie : Recommandations en lien avec des ressources organisationnelles***
  - ✓ Notifier aux potentiels clients et clients que leurs données font l'objet de traitement lors de l'exécution de contrat ou de pré-contractualisation (***règle n°1 : légalité du traitement***) ;
  - ✓ Définir le ou les finalités spécifiques du traitement en toute transparence (**précisément déterminée, explicite et légitime**) sans les altérer ou les modifier dans le temps sans l'aval des personnes concernées (***règle n°2 : Transparence et finalité du traitement***)
  - ✓ Limiter les **données collectées aux stricts nécessaires** et définir une **durée de conservation** de celles-ci tout en respectant le ***cycle de vie de la donnée*** (l'anonymisation des données, l'archivage et la suppression) (***règle n°3 : protection particulière et conservation limitée des données***)
  - ✓ Mettre en place une **sécurité adaptée** pour prévenir les risques d'atteinte de la sécurité des données collectées et traitées à travers **des mots de passes robustes pour sécuriser les accès et des accréditations pour limiter l'accès selon les besoins métiers** (***règle n°4 : obligation de sécurité***) ;
  - ✓ Rappeler à toutes les personnes concernées par la collecte des données qu'ils disposent des **droits d'accès, de rectification, de suppression, d'opposition, de portabilité, de limitation de traitement, de définir le sort des données après leur mort et de ne pas faire l'objet de décision automatisée** (***règle n°5 : droits des personnes***) ;

II. Règles d'or à instaurer pour une bonne gouvernance des données :

- ✓ Mise en place d'une stratégie Data au cœur de l'entreprise (orientation liant tous les services de l'entreprise dans un souci de modernité d'augmentation de productivité) ;
- ✓ Fixer des objectifs généraux et spécifiques pour évaluer l'efficacité les plans d'actions de la gouvernance (cela se fait par un ensemble d'objectifs précis et SMART) ;
- ✓ Définition d'indicateurs de performances encore appelés KPI (Key Performance Indicator) s'insérant avec harmonie à la stratégie des données ;
- ✓ Définition d'une charte ou d'un ensemble de règles évolutives lié à la qualité des données exploitées pour assurer une productivité efficiente de l'entreprise (registre de traitement, règle juridique, et les outils de traitement) ;
- ✓ Etablir des communications (internes comme externes) pour valoriser la nouvelle charte de gouvernance de la donnée (Ateliers de réflexions, entretiens, post, newsletter et d'autres)

Conclusion

Au regard des sanctions et des restrictions que connaît DEV'IMMEDIAT dans la délivrance de ces prestations, voici une petite liste de règles à intégrer dans le quotidien de l'entreprise (*la synthèse des recommandations*). Ces règles lui permettront ainsi de ne collecter et de traiter les données indispensables à leurs travaux tout en respectant les exigences liées aux normes du RGPD.

Toutefois, l'entreprise doit mettre un accent particulier sur son mode de collecte et de traitement de la donnée tout en rappelant à ces clients leurs droits dont ils disposent. De plus, ils doivent avoir leur consentement légal et éclairé tout en mettant en place les dispositifs de sécurité et de périodicité en rapport avec la conservation des données