Recommandations sur le traitement des données Dev'Immediat

Version	Auteur	Description	Date
V1	Nathalie Currid	Règles de gestion à mettre en place sur les données du CRM (Customer Relationship Management) pour une mise en conformité au RGPD	21/02/2024

Introduction

Dev'Immediat est un courtier en assurance automobile dont le métier est de faire de la prospection commerciale et de la marge sur la vente de contrats d'assurance automobile, en réponse à des demandes de devis faites en ligne. Suite à l'utilisation d'anciennes données de prospection commerciale pour l'établissement d'un devis, la CNIL a sanctionné Dev'Immédiat avec une limitation temporaire de 6 mois du traitement des données personnelles de ses clients. A l'issue de ces 6 mois, l'entreprise devra prouver que le traitement de ses données est dorénavant conforme aux normes RGPD (Règlement Général sur la Protection des Données), afin que la sanction soit levée.

A l'heure actuelle :

- Il n'y a pas de processus en place pour permettre aux clients d'avoir accès à leurs données personnelles ;
- Les données anciennes ne sont pas supprimées ni archivées, ce qui pose problème car :
    - L'entreprise ne respecte pas la règle de conservation limitée des données (règle 5),
    - Les nouveaux devis peuvent être biaisés car basés sur des données erronées ;
- Certaines données du CRM, dont une partie de nature sensible, n'ont pas de finalité spécifique qui soit liée à l'activité de l'entreprise (No de SS, groupe sanguin), de ce fait :
    - Les règles 3 et 4 de conformité au RGPD ne sont pas respectées ;
- Les données relatives à la prospection et aux demandes de devis sont accessibles par tous les membres de l'entreprise alors que certains services n'en ont pas l'utilité, il en résulte que :
    - L'entreprise ne respecte pas le principe de minimisation des données (règle 3),
    - La présence d'informations inutiles peut avoir un impact négatif sur la qualité du travail des équipes.

Une équipe a été constituée pour déterminer :

A **Quelles sont les mesures à mettre en place pour permettre à l'entreprise de continuer à exercer son activité pendant ces 6 mois de sanction ?**

Il a été décidé de mettre à disposition de l'équipe de performance commerciale une extraction des données anonymisées du CRM, au format CSV, avec des données tarifaires non détaillées (voir rapport s'y référant).

B **Quelles sont les actions correctives à mettre en place pour être en conformité avec les normes RGPD, à l'issue des 6 mois, afin de demander une levée des sanctions ?** Ceci est l'objet des recommandations qui vont suivre.

Les bénéfices de ces actions, outre la levée des sanctions et la prévention seront :

- L'accès à une base de données 'propre' qui permettra une meilleure prospection du service commercial et la production de devis plus justes (amélioration du taux de satisfaction et du taux de conversion),
- Un gain en efficacité au niveau du traitement des données par les différents services concernés.

Les membres de l'équipe sont :

- Clara DAUCOUR, Directrice générale de Dev'Immédiat
- Jean Luc, DPO (Data Protection Officer) temporaire, Adjoint de la directrice
- Salomé SAQUE, Auteur du dictionnaire de données, base clients

DEV'IMMEDIAT

RECOMMANDATIONS SUR LA COLLECTE, LE TRAITEMENT ET LA DOCUMENTATION DES DONNÉES

1) **Définir la finalité du traitement des données par service dans l'entreprise**
   (prospection, devis, contrats, suivi et support clients)

2) **Évaluer la base de données actuelle**
   - Répertorier les données du CRM en vérifiant qu'elles correspondent bien à la dernière version du dictionnaire de données – Base client (v1.21 du 03/05/2022 – Salome Saque) ;
   - A partir de cet inventaire, identifier :
     - les données strictement nécessaires pour atteindre la finalité,
     - les données utiles à des fins statistiques mais ne nécessitant pas d'être reliées aux données des clients,
     - les données sensibles,
     - les données non nécessaires à la finalité.

3) **Minimiser les données, avec une attention particulière pour les données sensibles**
   - Supprimer les données non nécessaires à la finalité, particulièrement les données sensibles permettant une identification des clients, comme les données de santé (No de SS) ;
   - Modifier les outils de récolte des données afin de ne demander que celles nécessaires au traitement des demandes, de plus s'assurer que les personnes aient connaissance de leurs droits et puissent les exercer ;
   - Anonymiser les données utiles que Dev'Immediat souhaite garder à des fins statistiques et créer une table et un 'Dictionnaire de données – Statistiques' spécifiques (Salomé Saque) ;
   - Cloisonner les données en fonction de leur pertinence par service (Service prospection commerciale, Service clients).

4) **Établir le cycle de vie des données**
   - Définir la durée d'utilisation de chaque type de données selon qu'un contrat a été établi ou pas (prospects : 3 ans) ;
   - Déterminer les actions à mettre en place lorsqu'elles arrivent en fin de vie : archivage, anonymisation ou suppression ;
   - Mettre à jour le 'Dictionnaire de données – Base client' (Salomé Saque) avec la liste des données strictement nécessaires, en incluant :
     - La durée de vie de chaque type de donnée et le process une fois arrivé en fin de vie,
     - le type de données (integer, char, varchar) au lieu de string, la taille des données et les clés.

5) **Sécuriser les données**

Nommer/recruter un DPO permanent, en remplacement de Jean-Luc, afin de mesurer et prévenir les risques d'atteinte à la sécurité technique et organisationnelle des données (accès, stockage, sensibilisation des employés aux normes RGPD à travers des formations et la création d'une charte de gouvernance des données).

Conclusion

Il est important de noter qu'à l'avenir chaque donnée demandée devra être justifiée par une nécessité opérationnelle ou légale claire. De plus, les clients devront être informés des mesures prises pour protéger leurs données, conformément aux exigences du RGPD. Enfin, chaque membre de Dev'Immediat devra être sensibilisé aux normes du RGPD et développer des bonnes pratiques de traitement des données en se référant à la charte de gouvernance des données qui sera créée.