Recommandations sur les règles de gestion à mettre en place sur les données du CRM pour être conforme au RGPD Dev'Immediat :

Recommandation 1) Mise en place d'une vraie politique de gestion de protection des données de bout en bout chez Dev Immédiat.

- Comme le mentionne Clara, Dev'Immediat n'a actuellement aucun processus pour gérer les demandes clients accéder à ses données personnels sensibles, les rectifier et les supprimer. Avant tout, il faut donc mettre en place une politique complète de protection des données RGPD chez Dev Immédiat décrivant les process et démarches à suivre, la communication, la documentation et la formation de l'équipe dédiée à la mise en œuvre et de la maintenance de celle-ci.
- Ceci inclut également l'élection d'un DPO officiel en replacement du rôle temporaire de Jean Luc .

Recommandation 2) Etablir un traitement sur les données personnelles conformes au RGPD afin de faciliter le partage des données entre service nécessaires aux différentes analyses internes

- Un traitement d'anonymisation doit être mis en œuvre pour protéger la confidentialité des individus et éviter la divulgation d'informations sensibles ou confidentielles tout en permettant l'exploration et la prise de décision basée sur les données.
- Ainsi des tranches de valeurs plutôt que des valeurs explicites doivent être mise en place pour masquer et anonymiser les données : la date de naissance précise des clients doit être remplacée par des catégories générales : Jeune : moins de 25 ans / Adulte : 25-64 ans / Senior : 65 ans et plus), le nb d'enfant en conduite accompagné, le nombre de point du permis perdus…

Recommandation 3) Mettre la base de données du CRM conforme au RGPD au niveau de la collecte.

- Une étude détaillé doit être menée pour ne sélectionner que les données strictement nécessaires et collectées pour le domaine de l'assurance auto (comme l'usage du véhicule, la Tranche de kilomètre parcouru par an, la Motorisation du véhicule, la puissance…), des infos obsolètes des années 80 comme la couleur rouge de la voiture doivent être supprimés.
- Les données sensibles qui ne peuvent être justifiées par les bases légales fixées par le RGPD Dev Immédiat ne doivent pas être collectées et être supprimées du CRM (par ex. numéro de Sécurité Sociale, le Groupe sanguin, le nom de l'employeur, …).Des catégories de données, surement nécessaire à des fins statistiques, sont trop intrusives et doivent être revues. Par exemple, le revenu doit être remplacé par des tranches de revenus et le métier pourrait être remplacé par des catégories socio-professionnelles.

Recommandation 4) : Mettre en place une communication claire et transparente avec le Client sur la collecte l'utilisation et le traitement de ses données personnelles ainsi que leurs droits afin qu'il donnent explicitement leur consentement.

- Mise en place d'un processus d'information (politiques de confidentialité) et de consentement clair (formulaires) et transparent lors de la saisie des informations du client sur le site web et le dépôt de cookies
- Expliquer sous forme d'accès pop-up quelles données sont collectées, l'équipe Dev'Immediat doit réfléchir à la finalité du pourquoi ces données sont collectées (est-ce par ex. pour établir le meilleurs tarifs d'assurance auto au plus près des usages quotidien ?) et comment elles sont utilisées (à des fins commerciales statistiques, suivi de dossier etc..).
- Il faut également informer les clients des droits dont ils disposent en matière de protection des données, tels que le droit d'accès, de rectification, d'effacement et d'opposition sur les données stockées dans le CRM Dev'Immediat

Recommandation 5) Mettre en place un processus de sécurisation des données personnelles des Clients stockées dans le CRM Dev'Immediat

- Afin de sécuriser et limiter les accès aux données personnels des clients, il faut que Dev'Immediat établisse un état des lieux de la sécurité des systèmes d'information accédant au CRM incluant la stabilité du système, les vulnérabilités en cas d'attaque, ou encore les risques en matière de disponibilité du serveur.
- Cela implique également de mettre en place des politiques d'accès spécifique pour chaque département dans l'entreprise par exemple cloisonner les accès a certaines information par département, limité les personnes habilités à accéder aux informations sensibles, sécuriser l'accès au CRM avec une politique de mot de passe à authentification à deux facteurs, le cryptage des données CRM …
- Dev'Immediat doit donc mettre en place des procédures et des mesures de sécurité organisationnelle mais également de contrôles et sensibilisations des équipes pour garantir le niveau de sécurité des données personnel de ses clients pour prévenir tout accès non autorisé, toute divulgation ou toute perte de donnée.

Recommandation 6) Mettre en place un processus d'archivage de la base de données du CRM

- Comme le mentionne Clara, Dev'Immediat, les anciennes données de prospection commerciale d'un client datant de plus de 7 ans ont été conservées et ont mis en péril l'activité de Dev'Immediat. Il faut donc établir une politique stricte d'archivage et de suppressions des données obsolètes.
- Dès que la finalité pour laquelle les données ont été collectées est atteinte il faut que Dev'Immediat établisse une durée de vie en prenant en compte les besoins de chaque service pour l'archive et la suppression des données (par exemple pas plus de données de plus de 3 ans dans les données transmise au service commercial).