Recommandations

Réaliser un AIPD.

Au vu des données à haut risque présent dans la base comme numéros de sécurité sociale, données de santé, salaire et adresse précise, il faudrait effectuer une Analyse d'impact relative à la protection des données.
Dans un premier temps il faudrait évaluer l'accès au donnée, quel service fait quoi et quels sont les données uniquement pertinentes que chaque service à besoin. Cela nous permettra de cloisonné logiquement les données dans le CRM, mais ça on y reviendra plus tard.
Puis identifier les risques, comme la fuite de données ou un profilage très intrusif.
Une fois ceci fait on liste les mesures existantes puis on propose les mesures complémentaires.
L'avantage c'est que cela permet de mettre ne évidences les risques, planifier une feuille de route et mettre à jours le registre. Mais le plus important cela peut servir de preuve vis-à-vis de la CNIL en cas de contrôle.
Le désavantage c'est que cela prend du temps et mobilise des ressources IT importante et la nécessité pour faciliter les traitements d'avoir un DPO. Ceci dit, avec la sanction de 6 mois de la CNIL cela nous donne le temps de gérer cela tout en mettant au normes le traitement des données.

Gouvernance des données et cycle de vie.

Il faut créer une charte pour le cycle de vie des données stocké dans le CRM. Pour ce il faut dès la collecte définir si les données sont licite et cohérente avec l'exigence métier, combien de temps peut on les stocker et le mode opératoire de chaque étape de la vie des données (collecte, exploitation, archivage, anonymisation et suppression). Une fois l'état des lieux fait on rédige une charte que l'on tien a jours selon l'évolution du logiciel métier et ou des usages commerciaux, puis on la traduit en règles techniques comme des script de purge automatique ou un workflow d'anonymisation pour les comptes inactifs.
L'avantage c'est que l'on s'alignes sur les principes RGPD tout en facilitant les réponses aux demandes des différents collaborateur et ou client. Cependant il y a des désavantage comme trouver le bon compromis entre exigences RGPD et besoin métier (ici on supprime les « ça peut peut-être servir »).

Organisation des droit d'accès et cloisonnement logique.

Ici on limite l'accès aux données d'un même ID client selon le besoin métier. Que ce soit la partie auto, santé, crédit immo, comptabilité … Chacun peut avoir l'accès au compte du client et de ces données mais uniquement à celle qui sont pertinente par rapport au besoin métier de celui qui le consulte. Pour cela il faut cartographier les besoin métier de chaque

secteur de l'entreprise, mais cela sera déjà fait pendant les deux premières recommandations. L'avantage c'est que cela empêche le profilage abusif et la curiosité mal placé entre service est créer une première couche logique de sécurité en cas de compte compromis.

Renforcement de la sécurité du CRM.

Cette fois ci on passe à la deuxième couche de protection logique en deux points. Le premier c'est le chiffrement de la base, pour que si cette dernière est dérobée, soit totalement inutilisable. Double avantage ici on sécurise les données client ce qui donne une forte confiance du client vis-à-vis de la société mais aussi cela réduit les risques d'avoir des sanctions de la CNIL.
Deuxième points, l'authentification forte. Pour réduire cette fois le risque de compromissions des compte utilisateurs des collaborateurs, la mise en place d'une authentification forte évite les accès ç la base en clair via un compte dérobé à un de vos collaborateur. Pour ce point deux éléments important un mot de passe robuste avec majuscule minuscule et caractère spéciaux d'au moins 12 caractères et une double authentification via code OTP sur une application comme authentification.
Pour sensibiliser vos équipes et si vous avez un DSI vous pouvez faire des campagnes de sensibilisation avec des faux mail de phishing.

Mise en place d'une stratégie de sauvegarde.

Ici on passe à la partie de cloisonnement à la fois physique et logique. Ce parti est aussi subdivisé en plusieurs éléments. Premier point une sauvegarde de la base sur un autre serveur pour avoir un backup avec les mêmes niveaux de sécurité que les précédents. Ce qui permet en cas de panne, incident technique, vol, piratage de reprendre rapidement une activité. Une Double sécurité peut être aussi faite sur un support externe ce qui le protège des ransomware, même si cela ne vous dispense pas d'avoir un anti ransomware. Puis pour tout ce qui est Archives le mieux c'est qu'une fois les process de gouvernance appliqué vous gardez une archive sur un support externe sécurisé entreposé dans une sale d'archive sécurisé.
Une fois tout les X temps selon le type de données vous devez effectuer une purge des archives et sauvegarde, surtout si ces dernières sont journalisées et conserve en l'état des sauvegarde antérieures.

Pour terminer plus qu'une recommandation c'est une obligation, il faut faciliter aux clients l'exercice de leurs droit via un formulaire simple, clair et facile d'accès.