RECOMMANDATIONS POUR ETRE CONFORME AU RGPD

Le Règlement général sur la protection des données (RGPD) est une loi européenne qui vise à protéger les données à caractère personnel des citoyens de l'Union européenne (UE) et à garantir leur confidentialité et leur sécurité. Pour être en conformité avec le RGPD en ce qui concerne les données du CRM, Dev'Immediat doit mettre en place les règles de gestion suivantes :

1. Obtenez un consentement explicite et éclairé

L'une des principales exigences du RGPD est d'obtenir un consentement clair et éclairé des personnes dont les données sont collectées. Cela signifie que vous devez obtenir leur consentement de manière explicite et informée, en leur expliquant clairement pourquoi vous collectez leurs données, comment vous les utilisez et comment elles peuvent exercer leurs droits en matière de protection des données. Les personnes doivent être informées de manière claire et précise de la finalité de la collecte de données. Assurez-vous que vos formulaires de consentement sont faciles à comprendre et que les personnes peuvent les accepter ou les refuser facilement. Les données personnelles collectées doivent être limitées à ce qui est strictement nécessaire ou anonymisées pour atteindre l'objectif de traitement.

2. Mettez en place des mesures de sécurité appropriées

Le RGPD exige que vous mettiez en place des mesures de sécurité appropriées pour protéger les données à caractère personnel contre tout accès non autorisé, la perte ou la divulgation. Cela peut inclure la mise en œuvre de pare-feu, de cryptage des données, de protocoles d'authentification robustes et de contrôles d'accès appropriés. Pouvez appliquer la méthode EBIOS proposée par ANSSI (Agence nationale de la sécurité des systèmes d’information) qui consiste à identifier et quantifier les scénarios de cyberattaque critique, et à préparer une stratégie de sécurité. Vous devrez également vous assurer que vos employés sont formés à la protection des données et que vous avez mis en place des procédures pour détecter, signaler et gérer les incidents de sécurité.

3. Respectez les droits des personnes concernées

Le RGPD confère aux personnes concernées certains droits en matière de protection des données, tels que le droit d'accéder à leurs données, de les rectifier, de les effacer, de s'opposer à leur traitement et de les transférer. Vous devrez mettre en place des procédures internes pour vous assurer que vous pouvez respecter ces droits dans les délais impartis par la loi. Vous devrez également informer les personnes de leurs droits en matière de protection des données et de la manière dont elles peuvent les exercer.

4. Conservation limitée des données

La conservation des données à caractère personnel est soumise à des limitations légales en France et dans l'Union européenne (UE) en vertu du Règlement général sur la protection des données (RGPD). Il est important de noter que la conservation des données à caractère personnel doit être justifiée et limitée dans le temps, conformément aux principes énoncés par le RGPD, afin de protéger la vie privée et les droits des individus. Dès que la finalité pour laquelle elles ont été collectées est atteinte, les données selon les cas peuvent être : **archivées, supprimées, anonymisées et minimisées.** Dans tous les cas, une durée de conservation doit être définie et appliquée.

5. Évaluez et documentez votre conformité

Il est important d'évaluer régulièrement votre conformité au RGPD et de documenter vos efforts en matière de protection des données. Vous devrez effectuer des évaluations d'impact sur la protection des données (EIPD) pour les traitements de données, tenir des registres de vos activités de traitement, et vous assurer que vous avez les documents nécessaires, tels que des politiques de confidentialité et des accords de traitement des données.