REGLES DE GESTION POUR CONFORMITE RGPD

Voici une liste de recommandations concernant les règles de gestion à mettre en place sur les données CRM afin d'être conforme au RGPD.

Tous d'abord, la décision de former une équipe dédiée est judicieuse. Cette équipe sera en mesure de garantir le suivi des recommandations émises ci-dessous, de fournir des interlocuteurs spécifiques pour toute demande d'information, qu'elle soit interne ou externe, de créer de la valeur grâce à une stratégie data alignée à celle de l'entreprise et de garantir sur le long terme la conformité aux règles RGPD.

- La minimisation des données :

Uniquement les données essentielles et nécessaires pour atteindre l'objectif fixer à ce traitement peuvent être collecté.

Par exemple connaitre le groupe sanguin de nos clients n'a pas d'intérêt dans la gestion des contrats.

Attention il faut porter également une attention particulière sur les données dite sensibles (concernant la santé, les opinions politiques, religieuses, ...) qui ne peuvent être collectées et traitées que dans certaines conditions. Le RGPD interdit de recueillir ou d'utiliser ces données, sauf dans certains cas qui sont précisément listés (cf. Art. 9 du RGPD).

- La conservation limitée des données :

Il est impératif de déterminer une durée de conservation des données et de l'appliquer rigoureusement. Une fois que l'objectif initial de leur collecte est atteint, les données peuvent être soit archivées, supprimées, ou anonymisées.

Ici on préféra choisir une anonymisation afin que le service performance commerciale puisse effectuer leur analyse. Un an après la collecte des données par l'équipe commerciale semble être un délai raisonnable.

- La sécurité des données :

Les entreprises sont tenues de mettre en place des mesures de sécurité appropriées pour protéger les données personnelles contre tout accès non autorisé, toute divulgation, toute altération ou toute destruction accidentelle ou illicite via :

-une sécurisation technique : le cryptage, les pare-feu et les antivirus.

-une sécurisation organisationnelle : En plus des mesures techniques, adopter des politiques et des procédures internes pour garantir la sécurité des données, telles que des contrôles d'accès stricts et des formations en matière de sécurité pour le personnel.

-une gestion des risques : mener des évaluations régulières des risques pour identifier les menaces potentielles

-une notification des violations : En cas de violation de données personnelles, notifier l'autorité de contrôle compétente dans les 72 heures suivant la découverte de la violation, sauf si la violation n'est pas susceptible de présenter un risque pour les droits et libertés des individus concernés.

- Transparence et droits des personnes :

Les personnes doivent être informées de l'utilisation faites des informations récolter les concernant et la manière dont ils peuvent exercer leurs droits leurs permettant de garder la maitrise de leurs données. Le droit d'accès, le droit de rectification, le droit de suppression, le droit d'opposition, le droit à la portabilité, le droit à la limitation du traitement, le droit de définir le sort des données après la mort, le droit de ne pas faire l'objet d'une décision automatisée.

- La création du registre des activités de traitement :

L'article 30 du RGPD stipule l'obligation pour les responsables du traitement des données de maintenir un registre de leurs activités de traitement. Il doit contenir des informations détaillées sur les activités de traitement des données personnelles effectuées par l'organisation. Cela inclut notamment les finalités du traitement, les catégories de données personnelles traitées, les destinataires des données et les mesures de sécurité mises en place. Le registre est également un outil de responsabilisation pour les responsables du traitement. Il leur incombe de maintenir ce registre à jour et de le tenir à la disposition de l'autorité de contrôle compétente en cas de demande. Il a aussi pour but de contribuer à accroître la transparence des activités de traitement des données au sein de l'organisation. Il permet aux individus de comprendre comment leurs données sont utilisées et traitées.

Le registre de l'activité de traitement est un outil essentiel pour les responsables du traitement afin de documenter et de démontrer leur conformité aux obligations en matière de protection des données.