Recommandations sur les règles de gestion à mettre en place sur les données du CRM

Vous avez fait appel à nous afin de mettre en place des actions correctives à la suite des sanctions établies par la CNIL. En effet, sans action de votre part, vous ne pourrez utiliser les informations personnelles de vos clients pendant 6 mois et votre activité en sera fortement impactée.

J'ai pu établir 5 recommandations d'actions à prévoir pour être conforme aux règlementations du RGPD

- Mettre en place un plan d'action de gouvernance de données

La première étape dans la mise en place de la gouvernance de vos données est d'affecter un DPO (délégué à la protection des données) pour piloter la mise en conformité au RGPD.

Vous nous avez donc informés que Jean-Luc, votre adjoint sera le DPO.

En effet, vous souligner ne pas avoir de collaborateurs en mesures de répondre aux questions de conformité et de données clients.

- Suivre la méthode DAMA-DMBOK (Data Management Body of Knowledge), et sa fameuse « roue DAMA » en sécurisant les données avec un degré de sécurité approprié selon la nature de la donnée.
- Permettre une interopérabilité des données afin de pouvoir les déplacer et les communiquer entre plusieurs systèmes sans problème de compatibilité.
- Stocker les données
- Gérer la qualité des données et leurs capacités à être utilisée par les utilisateurs.
- Il faudra donc récupérer la donnée, l'identifier, la sécuriser, puis lui donner de la valeur en la rendant plus cohérente et donc plus qualitative.
- Il faudra maitriser le stockage des données et leurs cloisonnements

- Mettre en place un plan de communication en sensibilisant les collaborateurs.

Instaurer une culture interne de la sécurité en identifiant les mauvaises pratiques des collaborateurs, former en interne.

Déterminer les menaces fréquentes en cybersécurité, tels que les rançongiciels, les attaques DDoS qui visent à déstabiliser le système informatique, l'hameçonnage, et enfin le risque humain.

Il faut identifier les mesures applicables et accessibles à tous telles que la sécurisation des mots de passe, verrouillage des postes de travail, délimiter la vie professionnelle et personnelle des collaborateurs.

- Sécuriser juridiquement et techniquement les données

Effectuer un audit externe afin d'avoir un état des lieux de la sécurité des systèmes d'information, déceler si les outils informatiques utilisés répondent bien au besoin de votre entreprise., mesurer la stabilité du système, la vulnérabilité en cas d'attaque.

Réalisation de tests de sécurité pour évaluer le degré de sécurité en fonction des données et de leur sensibilité.

Respecter la norme ISO/IEC 27001 est la norme de référence ; elle impose certaines exigences de sécurité de base pour préserver l'intégrité, la disponibilité et la confidentialité des données.

- Améliorer la qualité des données

Actualiser les données pour qu'elles soient toujours à jour au moment où vous voudrez les utiliser
Sécuriser les données et les rendre conformes aux règles de droit en vigueur.
Tracer les données tout au long de leurs cycle de vie, savoir les manipuler et quand les supprimer.
Classer les données et s'assurer qu'elles soient complètes et précises pour faciliter les taches des collaborateurs.

- Respect des règles juridiques

Etablir le registre des activités de traitement de la société qui regroupe l'ensemble des acteurs intervenants dans le traitement des données, la catégorie des données, leur durée de conservation, leurs fonctions, les personnes qui accèdent à ces données et les raisons pour lesquelles elles en disposent.

L'aspect juridique, la base légale, c'est-à-dire le consentement des clients, les raisons pour lesquelles les données sont collectées, les délais de conservation et la sécurité mise en place.