Projet n°4 Formation Business Analyst

A la demande du client, et en tenant des données sensibles que récolte l'entreprise, voici cinq recommandations pour renforcer la conformité RGPD :

1. Limiter la collecte des données aux informations strictement nécessaires

Conformément à la règle de minimisation des données, on recommande de revoir la base de données et de restreindre la collecte aux informations essentielles pour les analyses. Par exemple, le groupe sanguin et le numéro de sécurité sociale ne sont pas indispensables pour les contrats d'assurance, il faut les supprimer.
Cette approche permet de réduire les risques associés au traitement de données sensibles.

2. Définir clairement les finalités des données récoltées

Chaque donnée collectée doit être associée à une finalité explicite et légitime.
Définissez ces finalités, et communiquez-les clairement aux clients, en précisant pourquoi chaque information est requise et comment elle sera utilisée.
Par exemple, les informations de revenus et de résidence peuvent être justifiées pour évaluer les risques en assurance, mais pas pour des usages promotionnels non prévus initialement.

3. S'assurer le consentement pour les données sensibles

Pour les données sensibles (santé, informations financières), il convient d'obtenir un consentement explicite des clients. Ce consentement doit être libre, spécifique et informé. Il est alors utile de prévoir des mécanismes de traçabilité de ce consentement pour prouver la conformité en cas de contrôle.

4. Mettre en place une politique de conservation des données

Limitez la durée de conservation des données en fonction de leur finalité. Par exemple, les informations relatives aux devis non conclus peuvent être supprimées ou anonymisées après un délai défini (ex. 2 ans), tandis que les informations de clients actifs peuvent être conservées tant que le contrat est en d'actualité.

5. Renforcer les mesures de sécurité et les contrôles d'accès

Conformément à l'obligation de sécurité, mettez en place des mesures comme le chiffrement des données sensibles (numéro de sécurité sociale, adresse, informations financières) et des contrôles d'accès stricts pour garantir que seules les personnes autorisées peuvent accéder aux données personnelles (Groupes AD, RLS etc.).