RGPD – 4 actions principales

Pour vous mettre en conformité, la CNIL a identifié 4 actions principales à mener et à poursuivre dans le temps.

ACTION 1 : Recensez vos fichiers pour les intégrer au registre de traitements des données

Il faut ici identifier toutes les activités de l'entreprise qui nécessitent de collecter et traiter des données puis créer une fiche pour chaque activité recensée en l'incluant dans un document général, le registre des traitements

Dans ce registre, vous n'avez pas à mentionner les traitements purement occasionnels (fichier client constitué pour l'envoi d'une invitation à l'inauguration d'un local par exemple)

ACTION 2 : Faites le tri dans vos données

Pour chaque fiche d'activité, **vérifiez que les données collectées sont nécessaires** : avez-vous besoin de la date de naissance d'un prospect ou d'un client. Avez-vous besoin de connaitre le nombre d'enfants de vos salariés ?

Vérifiez également que vous ne conservez pas des données au-delà de ce qui est nécessaire.

La mise en conformité est l'occasion de réfléchir à la pratique de l'entreprise en minimisant la collecte de données.

ACTION 3 : Respectez les droits des personnes

Le RGPD renforce l'obligation d'information et de transparence à l'égard des personnes sont vous traitez les données, il est indispensable d'inclure dans tous les supports utilisés pour collecter des données un certain nombre de mentions :
Pourquoi les données sont collectées ? Etablir un contrat par exemple
Ce qui autorise à collecter les données ? Obligations légales pour des déclarations sociales par exemple ;
Qui a accès aux données en interne ? la secrétaire comptable par exemple ;
Comment la personne peut exercer les droits liés à ses données ? boite mail dédiée par exemple ;
Le temps de conservation des données ;

Il est indispensable d'assurer aux personnes la possibilité d'exercer leurs droits en mettant en place un processus interne pour garantir une réponse à la demande de la personne dans un délai court.

ACTION 4 : Sécurisez vos données

Il s'agit de prendre toutes les mesures nécessaires pour assurer la protection informatique ou physique de votre « patrimoine de données ».

Parmi les mesures à prendre : mettre à jour vos antivirus, changer régulièrement vos mots de passe, utiliser des mots de passe dits forts, mélangeant lettres, chiffres et signes
Mais aussi, stockez vos fichiers papier dans une armoire fermée à clé…

Cette réflexion autour de la sécurisation des données doit aussi porter sur la pratique en cas d'incident, de type piratage…

Si votre entreprise a subi une violation de données, **vous devez le documenter en interne**, c'est-à-dire créer un document qui conservera la trace de cette violation avec un certain nombre de mentions (nature de la violation, nombre de données concernées, conséquences, actions correctrices engagées)

Si cela apporte un risque pour les personnes concernées (données dites sensibles), vous devez en informer la CNIL (sur leur site) dans les 72 heures, voire informer les personnes concernées.