5 recommandations sur les règles de gestion.

1. Ne collectez que les données vraiment nécessaires

Posez-vous les bonnes questions : Quel est mon objectif ? Quelles données sont indispensables pour atteindre cet objectif ? Ai-je le droit de collecter ces données ? Est-ce pertinent ? Les personnes concernées sont-elles d'accord ?
Identifiez les activités principales de votre entreprise qui utilisent des données personnelles.
Exemples : recrutement, gestion de la paye, formation, gestion des badges et des accès, statistiques de ventes, gestion des clients prospects, etc.

Dans votre registre, créez une fiche pour chaque activité recensée, en précisant :

- L'objectif poursuivi (exemple : la fidélisation client) ;
- Les catégories de données utilisées (exemple pour la paie : nom, prénom, date de naissance, salaire) ;
- Qui a accès aux données (exemple : service chargé du recrutement, service informatique, direction, prestataires, partenaires, hébergeurs) ;
- La durée de conservation de ces données (durée durant laquelle les données sont utiles d'un point de vue opérationnel, et durée de conservation en archive).

Pour chaque fiche de registre créée, vérifiez que :

- les données que vous **traitez sont nécessaires à vos activités** (par exemple, il n'est pas utile de savoir si vos salariés ont des enfants, si vous n'offrez aucun service ou rémunération attachée à cette caractéristique) ;
- **vous ne traitez aucune donnée dite** « sensible » ou, si c'est le cas, que vous avez bien le droit de les traiter ;
- seules les personnes habilitées ont accès aux données dont elles ont besoin ;
- vous ne conservez pas vos données au-delà de ce qui est nécessaire.

À cette occasion, améliorez vos pratiques ! Minimisez la collecte de données, en **éliminant toutes les informations inutiles.** Redéfinissez qui doit pouvoir accéder à quelles données dans votre entreprise. Définissez, quand cela est possible, des règles automatiques d'effacement ou d'archivage au bout d'une certaine durée dans vos applications.

2. Soyez transparent

Une information claire et complète constitue le socle du contrat de confiance qui vous lie avec les personnes dont vous traitez les données.
Pour éviter des mentions trop longues au niveau d'un formulaire en ligne, vous pouvez par exemple, donner un premier niveau d'information en fin de formulaire et renvoyer à une politique de confidentialité / page vie privée sur votre site internet.

À l'issue de cette étape, vous avez répondu à votre obligation de transparence.

3. 3.Pensez aux droits des personnes

Vous devez répondre dans les meilleurs délais, aux demandes de consultation, de rectification ou de suppression des données.
Permettez aux personnes d'exercer facilement leurs droits

Les personnes dont vous traitez les données (clients, collaborateurs, prestataires, etc.) ont des droits sur leurs données : droit d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation du traitement.

Vous devez leur donner les moyens d'exercer effectivement leurs droits. Si vous disposez d'un site web, prévoyez un formulaire de contact spécifique, un numéro de téléphone ou une adresse de messagerie dédiée. Si vous proposez un compte en ligne, donnez à vos clients la possibilité d'exercer leurs droits à partir de leur compte.

Mettez en place un processus interne permettant de garantir l'identification et le traitement des demandes dans des délais courts (1 mois au maximum).

4.Sécurisez vos données

Les mesures de sécurité, informatique mais aussi physique, doivent être adaptées en fonction de la sensibilité des données et des risques qui pèsent sur les personnes en cas d'incident

Si le risque zéro n'existe pas en informatique, vous devez prendre les mesures nécessaires pour sécuriser les données.

Cela vous permet aussi de protéger votre patrimoine de données en réduisant les risques de pertes de données ou de piratage.

Les mesures à prendre, informatiques ou physiques, dépendent de la sensibilité des données que vous traitez et des risques qui pèsent sur les personnes en cas de d'incident.

Des réflexes doivent être mis en place : mettre à jour de vos antivirus et logiciels, bien choisir ses mots de passe, chiffrer vos données dans certaines situations et faire des sauvegardes.

Les failles de sécurité ont également des conséquences pour ceux qui vous ont confié des données personnelles : Ayez à l'esprit les conséquences pour les personnes et pour votre entreprise.

5.Identifiez les risques

a)Vous traitez énormément de données, ou bien des données sensibles ou avez des activités ayant des conséquences particulières pour les personnes, des mesures spécifiques peuvent s'appliquer. Effectuer un inventaire des données personnelles : il est important de savoir quelles données personnelles vous traitez, comment vous les traitez et où elles sont stockées. Cela vous permettra d'identifier les risques potentiels associés à chaque type de données et de mettre en place des mesures de sécurité adaptées.

b)Évaluer les flux de données : il est essentiel de comprendre comment les données personnelles circulent dans votre organisation, comment elles sont collectées, utilisées, stockées et transmises. Cela vous permettra d'identifier les points vulnérables de votre système et les risques potentiels associés à chaque étape du processus.

c)Identifier les menaces : il est important d'identifier les menaces potentielles pour la sécurité des données, telles que les cyberattaques, les vols de données, les erreurs humaines, les catastrophes naturelles, etc. Vous pouvez utiliser des scénarios de menaces pour identifier les risques potentiels et les conséquences associées à chaque scénario.