Protection des données : se mettre en conformité avec le RGPD (Cnil)

Si votre activité vous amène à collecter et à traiter des données personnelles pour votre compte ou pour le compte de votre entreprise (entreprise, association, collectivité…), vous devez vous conformer à la réglementation sur la protection des données.
Les obligations en la matière ont été renforcées, à compter du 25 mai 2018, avec l'entrée en application du Règlement général sur la protection des données (RGPD).

Qu'est-ce qu'une donnée personnelle ?
Il s'agit de toute information permettant d'identifier une personne physique directement ou indirectement :

- nom, prénom
- adresse mail
- carte de paiement
- numéro de téléphone
- identifiant (numéro client par exemple)
- numéro de sécurité sociale
- adresse IP
- photo d'un visage
- vidéo montrant une personne,
- etc.

A noter : l'identification d'une personne peut être réalisée à partir d'une seule donnée ou d'un croisement de plusieurs données.

Que faut-il entendre par "traitement de données personnelles" ?
Il est fait référence à toute action effectuée sur des données à caractère personnel de personnes physiques.

Exemples :

- collecte d'informations via une fiche de renseignements, un bordereau d'inscription, un questionnaire, un formulaire de contact, un formulaire d'inscription à une newsletter…
- enregistrement d'une base de données, d'un fichier clients par exemple…
- mise à jour d'un fichier fournisseurs,
- mise en place d'un système de vidéosurveillance…

Attention ! Certaines données sont dites "sensibles". Leur traitement nécessite de prendre des mesures supplémentaires. Il s'agit notamment du traitement de données :

- révélant l'origine raciale ou ethnique,
- portant sur les opinions politiques, religieuses ou philosophiques, sur l'appartenance syndicale,
- concernent la santé, l'orientation sexuelle,
- génétiques ou biométriques,
- portant sur des infractions et condamnations pénales.

Voir les informations et conseils de la Cnil à ce sujet

Comment vous mettre en conformité avec le RGPD ?
La Cnil vous recommande 4 actions principales à mener pour entamer votre mise en conformité :

1) Recensez l'ensemble de vos traitements de données dans un registre des activités de traitement (prévu par l'article 30 du RGPD).
Ce registre permet d'identifier précisément :

- les personnes qui interviennent dans le traitement des données,
- les catégories de données traitées,
- ce que vous faites de ces données,

- qui accède aux données,
- à qui elles sont communiquées,
- la durée de conservation des données,
- les mesures de sécurité mises en place.

La Cnil met à votre disposition un modèle de registre sous plusieurs formats.

A noter !
Les entreprises de moins de 250 salariés ne doivent inscrire sur ce registre que les traitements suivants :

- les traitements non occasionnels : gestion de la paie, fichiers clients, fichiers fournisseurs…
- les traitements susceptibles de comporter un risque pour les droits et libertés des personnes : vidéosurveillance, systèmes de géolocalisation…
- les traitements qui portent sur des données sensibles.

Par ailleurs, si vous opérez des traitements en tant que sous-traitant pour le compte de clients, vous devez mettre en place un second registre : le registre du sous-traitant.
Pour en savoir plus sur ce point, reportez-vous à l'article 28 du RGPD et au Guide du sous-traitant de la Cnil

2) Faites le tri dans vos données pour vérifier notamment que les données que vous traitez sont bien nécessaires à votre activité et que vous ne collectez pas de données sensibles.

3) Respectez les droits des personnes que vous sollicitez
Elles doivent en effet savoir ce que vous allez faire de leurs données, donner leur consentement au traitement et être en mesure d'exercer facilement leurs droits.
A chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit ainsi comporter certaines informations :

- identité et coordonnées du responsable du traitement (ou de son représentant),
- finalités du traitement effectué,
- base juridique du traitement,
- destinataires des données,
- durée de conservation des données,
- droit d'introduire une réclamation auprès d'une autorité de contrôle,
- etc.

A noter : la Cnil vous propose sur son site des modèles de mentions

4) Sécurisez vos données
Pensez à mettre régulièrement à jour vos logiciels et antivirus, changez régulièrement de mots de passe, etc.
Vous êtes en effet tenu à une obligation légale d'assurer la sécurité des données personnelles que vous détenez.
Que risquez-vous en cas de non-respect du RGPD ?
Un certain nombre de sanctions sont prévues. Elles ont été renforcées dans un souci de protection des personnes physiques sollicitées.
Elles varient en fonction de la gravité des violations notées par la Cnil : avertissement, sanction pécuniaire, injonction de cesser le traitement, retrait d'une autorisation accordée par la Cnil.
En savoir plus sur la procédure de sanction de la Cnil