Le Règlement Général sur la protection des données

Entre formulaires en ligne, enquêtes et inscriptions numériques, les données personnelles s'accumulent dans les bases de données des entreprises. Et si on faisait un petit rappel des règles que leur impose le Règlement Général sur la Protection des Données (RGPD)

Règlement Général sur la Protection des Données, de quoi parle- t-on ?

Le Règlement Général sur la Protection des Données (RGPD) poursuit trois objectifs principaux : permettre aux individus d'exercer un contrôle renforcé sur leurs données personnelles, responsabiliser les entités qui traitent ces données, et établir un cadre légal harmonisé de protection des données au sein de l'Union européenne.

- **Qui est concerné par le RGPD ?**

Le Règlement Général sur la Protection des Données (RGPD) s'applique à l'ensemble des organisations, qu'elles soient publiques ou privées, qui traitent des données personnelles pour leur propre compte ou pour le compte d'autrui, à condition qu'elles soient établies sur le territoire de l'union européenne ou que leurs activités visent directement les résidents européens.

- **Qu'est- ce- qu'une donnée personnelle ?**

Une donnée personnelle est toute information permettant d'identifier directement ou indirectement une personne (article 4 RGPD). Cela peut être :

- un nom ou prénom ;

- une adresse e-mail ;

- une photo ;

- une adresse IP ;

- Ou toute autre information pouvant identifier une personne.

Association Des Experts en Sécurité et Sûreté - ADESS
4, allée des Augustins 92390 Villeneuve-la-Garenne
contact@adess-fr.org
www.adess-eu.org

Si votre entreprise collecte, utilise ou stocke des données personnelles, il est fort probable que le RGPD s'applique à vous. Voici donc les principales règles à connaître et à respecter.

- **Les obligations clés des entreprises**

  - **Respecter le principe de licéité**

La licéité d'un traitement, correspond au fondement juridique qui autorise une organisation à collecter, utiliser et conserver des données à caractère personnel.

Pour être valable, un traitement de données doit reposer sur l'une des six bases légales prévues par le RGPD :

- Consentement ;

- Exécution d'un contrat ;

- Obligation légale ;

- Intérêt vital ;

- Mission d'intérêt public ;

- Intérêt légitime.

Concrètement, avant de collecter une donnée, une entreprise doit pouvoir répondre à la question suivante : Ai-je le droit de collecter cette information ? Ou sur quelle base légale je m'appuie?

L'absence de base légale rend le traitement illicite.

Exemple: Vous envoyez une newsletter commerciale à vos clients ? Le traitement est licite si vous obtenez préalablement leur consentement explicite.

  - **Définir une finalité précise et légitime**

La finalité d'un traitement de données désigne l'objectif pour lequel les données sont collectées et traitées. Les données doivent être collectées pour un objectif clairement défini dès le départ. En revanche, il est interdit de les collecter pour « plus tard » ou « on verra bien ».

Exemple : collecter les e-mails pour l'envoi d'une newsletter.

Concrètement, une finalité = un traitement

- **Appliquer le principe de minimisation**

Ne collecter que les données strictement nécessaires pour atteindre votre objectif.

Exemple: il n'est par exemple pas pertinent de collecter l'adresse postale, le numéro de téléphone et le statut matrimonial d'une personne pour l'envoi d'une newsletter, un prénom et une adresse e-mail suffisent. Collecter trop de données, c'est s'exposer inutilement.

- **Sécuriser les données**

Mettez en place des mesures techniques et organisationnelles pour protéger la confidentialité, l'intégrité et la disponibilité des données. Cela inclut la protection contre :

- les accès non autorisés ;
- les pertes accidentelles ;
- les fuites de données.

- **Définir une durée de conservation limitée**

Les données ne peuvent pas être conservées indéfiniment.

Le Règlement Général sur la Protection des Données impose que les données ne soient conservées que le temps nécessaire à l'objectif pour lequel elles ont été collectées.

Exemple : les CV des candidats non retenus lors d'un processus de recrutement ne doivent pas être conservés plus de 2 ans dans la CVthèque.

A l'expiration de ce délai, les données doivent être supprimées ou anonymisées.

Pour en savoir plus sur les durées de conservation et leurs modalités de mise en œuvre, veuillez consulter le site de la CNIL en suivant ce lien **Les durées de conservation des données | CNIL**

- **Informer clairement les personnes**

Les personnes concernées par les traitements de données doivent savoir comment et pourquoi leurs données sont utilisées. Cette information doit être simple, compréhensible et facilement accessible.

Chaque personne doit savoir :

- qui traite ses données ;

- pourquoi elles sont collectées ;

- combien de temps elles sont conservées ;

- a qui elles peuvent être transmises ;

- quels sont ses droits (accès, rectification, effacement, opposition, portabilité).

- **Faciliter l'exercice des droits**

Le RGPD garantit à chaque individu un véritable pouvoir sur ses données personnelles. Les entreprises doivent permettre aux personnes d'exercer leurs droits facilement et gratuitement.

Exemple : Un client qui ne souhaite plus recevoir de newsletters doit pouvoir se désabonner simplement et gratuitement via un lien dans l'e-mail ou une demande au service client.

- **Risques et bénéfices de la conformité**

- **Se conformer au RGPD, pourquoi c'est important ?**

Protéger les données personnelles n'est plus une option pour les entreprises : c'est une obligation légale et un impératif stratégique. Le RGPD impose des règles strictes pour garantir le respect des droits fondamentaux des individus, mais au-delà de la conformité, cette démarche instaure un véritable climat de confiance.

En sécurisant et en gérant rigoureusement les données, les organisations se prémunissent contre les sanctions, limitent les risques de cyberattaques et renforcent leur réputation. Mieux encore, elles cultivent la fidélité de leurs clients et se démarquent sur un marché où la protection de la vie privée est devenue un critère déterminant dans le choix des consommateurs et des partenaires.

- **Bonnes pratiques : audit et mise à jour réguliers**

- Nettoyez régulièrement vos bases de données

- Vérifiez vos formulaires et mentions d'information

- Réalisez des audits internes et mettez à jour vos procédures

Une démarche proactive évite bien des risques et montre votre engagement envers la protection des données.

Références:

- Règlement (UE)2016/679 du parlement européen et du conseil du 27 avril 2016 : Règlement - 2016/679 - FR - rgdp - EUR-Lex

- CNIL, RGPD : par où commencer ? | CNIL

- CNIL, Cybersécurité : les bénéfices économiques du RGPD | CNIL

Anonyme