GDPR: General Data Protection Regulation

LE GDPR, C'EST QUOI ?

Le GDPR, General Data Protection Regulation (en Français on parle de RGPD ou ‘’Règlement général sur la protection des données”), est une nouvelle législation européenne sur la protection de la vie privée qui entrera en vigueur le 25 mai 2018.

QUI EST CONCERNE PAR LA LEGISLATION ?

Toutes les entreprises et organisations basées en Europe qui collectent des données sur les citoyens européens, indépendamment de leur présence physique dans le pays concerné. Par 'toutes', il faut entendre toutes les entreprises indépendamment de leur taille (PME. Grandes entreprises, micro entreprises) ou de leur forme juridique (**ASBL, SA, Associations de Fait, etc**.).

POURQUOI EST-CE IMPORTANT ?

Les amendes en cas de violation du RGPD seront de 4% du chiffre d'affaires annuel mondial total de l'exercice précédent ou de 20 millions euros, le montant le plus élevé étant retenu.

QUELQUES CONCEPTS CLES QU'IL FAUT MAITRISER

DONNÉES PERSONNELLES :
Toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement : nom, numéro d'identification, localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

DONNÉES SENSIBLES :
Certaines données personnelles sont plus sensibles que d'autres. Il s'agit, par exemple, d'informations relatives à la race, la santé, les opinions politiques, les convictions religieuses ou philosophiques, l'affiliation à un syndicat, les préférences sexuelles ou le passé judiciaire. **Ces données ne peuvent être ni collectées, ni enregistrées, ni même demandées !**

QUELS SONT LES GRANDS PRINCIPES DE CETTE LEGISLATION ?

PRINCIPE I : LAICITÉ ET TRANSPARENCE
Il faut utiliser les données en justifiant son utilisation par une base légale, tout en étant transparent. Par exemple, justifier la collecte des données via un document relatant des finalités d'usage de celles-ci (conditions générales)

PRINCIPE II : CONSENTEMENT
Le consentement est défini comme "toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Cela signifie aussi que la personne peut, à tout moment, retirer son consentement, et ce, sans conditions.

PRINCIPE III : LE DROIT À L'OUBLI ET À L'ACCÈS DE SES DONNÉES
La personne a le droit de demander l’effacement et la suppression de ses données personnelles.
Les organisations peuvent refuser de supprimer les données pour des raisons particulières : droit de liberté d’expression et d’information, obligation légale pour la réalisation d’une mission d’intérêt public ou relevant de l’exercice de l’autorité publique.

Les données peuvent être transférées d’un prestataire à un autre. Par exemple, si un membre décide de s'affilier dans une autre organisation, il a le droit de vous demander de transférer toutes ses informations vers l'autre organisation.

PRINCIPE IV: LIMITATION DES FINALITÉS
Il faut impérativement s'assurer que les données encodées et sauvées sont utilisées à des fins explicites, spécifiques, légitimes pour aucun autre objectif que celui mentionné de manière publique et transparente.

Les données doivent être utilisées de manière sécurisée (un superviseur doit implémenter des mesures organisationnelles et techniques pour protéger les données contre leur destruction, perte, altération, divulgation ou accès…) On doit donner la priorité à la minimisation des données, aux restrictions d'utilisation et à la non-distribution des données à d'autres personnes sans une vérification des intérêts.

PRINCIPE V: EXACTITUDE DES DONNÉES
Les données à caractère personnel doivent être exactes et tenues à jour. Toutes les mesures doivent être prises pour que les données qui sont inexactes, soient effacées ou rectifiées sans tarder.

PRINCIPE VI: INTÉGRITÉ ET CONFIDENTIALITÉ
Les données doivent être utilisées de manière sécurisée (implémenter des mesures organisationnelles et techniques pour protéger les données contre leur destruction, perte, altération, divulgation ou accès…)

PRINCIPE VII : RESPONSABILITÉ
Le responsable du traitement des données doit être capable de démontrer que les prescrits du RGPD sont respectés.

PRINCIPE VIII : AUTOMATISATION
Les personnes ont le droit de ne pas être soumises à des décisions automatisées. Les organisations seront obligées d'assurer qu'un individu obtienne une intervention humaine, puisse exprimer son point de vue, reçoive une explication et conteste la décision.

QUELS IMPACTS POUR LES LIONS CLUBS ?

Règlementation applicable aux clubs et *de facto* aux membres (cf. consentement)

Respect de ce que les personnes ou membres veulent ou ne veulent pas.

Promotion pour les activités

- Toujours donner la possibilité de "se désinscrire" et ceci dès maintenant en mentionnant le texte suivant dans vos mails :

NB : Vous faites partie des ami(e)s et connaissances du Lions Club de _____. C'est à ce titre que vous recevez ce courriel. En fonction des nouvelles dispositions européennes (RGPD), si vous ne souhaitez plus recevoir de message de notre part, envoyez-nous, par retour de courriel, ce souhait. Nous en tiendrons évidemment compte.

- Seules les adresses e-mail du directory peuvent être utilisées pour des activités Lions.

Sécurité = obligation

- TOUJOURS utiliser des mots de passe sécurisés,
- Ne partagez pas vos données avec des personnes étrangères au Lions,
- N'envoyez pas de fichiers Excel avec des données personnelles par mail,
- Mettre les gens en "BCC" lorsque vous envoyez un courriel à un groupe,
- Partager des fichiers via une plateforme sécurisée, i Cloud, Dropbox, (notez que Microsoft OneDrive personnel n'est pas crypté),
- Utilisez www.wetransfer.com ou prenez un compte mail à www.protonmail.com pour envoyer des fichiers au lieu de courrier ordinaire.