



Liges et Comités régionaux d'Ile-de-France

Gentilly, le 16 avril 2018

Objet : Note juridique sur le Règlement Général de Protection des Données (R.G.P.D.)

À la demande des : Ligues et Comités Régionaux d'Ile-de-France

Affaire suivie par : Emile BENIZEAU

Courriel : emile.benizeau@crosif.fr

Tel : 01 49 85 84 99

À l'attention des Ligues et Comités Régionaux d'Ile-de-France.

Nous faisons suite à la demande de plusieurs Ligues et Comités qui ont sollicité des renseignements approfondis sur le Règlement (européen) Général de Protection des Données (R.G.P.D.) n° 2016/679 du 27 avril 2016, lequel sera applicable à compter du 25 mai 2018, pour mise en conformité avec ses dispositions par les organisations concernées dont les associations.

Le R.G.P.D. concerne la protection des données personnelles et vient remplacer les missions attribuées à la C.N.I.L. (la Commission Nationale de l'Informatique et des Libertés), autorité administrative indépendante de protection des données en France.

La réforme de protection des données poursuit trois objectifs :

- 1) Renforcer les droits des personnes, notamment, par la création d'un droit à la portabilité des données personnelles
- 2) Responsabiliser les acteurs traitant des données
- 3) Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données (notamment, transnationales)

À la date du 25 mai 2018, les organisations devront, *a minima*, avoir entrepris les démarches pour se mettre en conformité avec le R.G.P.D. Il s'applique aux acteurs économiques et sociaux, les entreprises évidemment, mais aussi les associations, les administrations et les collectivités ...

Ce règlement, comme tout règlement européen, sera directement applicable et obligatoire dans tous ses éléments dans les 28 États membres de l'Union Européenne et leur législation nationale.

A) Qu'est-ce qu'une donnée personnelle ?

Le R.G.P.D., dans son article 4, définit une donnée personnelle comme étant « toute information se rapportant à une personne physique identifiée ou identifiable (...) directement ou indirectement ».

Un simple nom est donc déjà une donnée personnelle.

Il existe donc une liste infinie de données personnelles qui peut aller de l'adresse postale, la taille, ou la photo d'une personne jusqu'à des données économiques, sociales, culturelles ou génétiques.

B) Les grands principes du R.G.P.D.

Vous devrez donc intégrer les 6 nouveautés apportées par le R.G.P.D. pour les informations déjà stockées et les informations que vous stockerez à l'avenir sur vos adhérents, bénévoles, donateurs, et autres membres :

1. Le renforcement des droits des personnes : il impose de recueillir et conserver le consentement des personnes au traitement des données personnelles.
2. L'obligation d'information : il impose aux structures victimes d'un piratage des données personnelles d'informer dans les 72 heures la Commission Nationale de l'Informatique et des Libertés (C.N.I.L.) et les personnes concernées dont les informations ont été volées.
3. Des sanctions lourdes : il met en place des sanctions dissuasives, pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires.
4. Le principe de minimisation des données collectées : il impose de ne collecter que les renseignements strictement nécessaires au regard des finalités pour lesquelles elles sont traitées.
5. Le droit de portabilité des données : les personnes, dont les informations ont été collectées, ont le droit de demander à recevoir les données à caractère personnel les concernant.
6. Le registre des données : il oblige les structures à tracer l'ensemble des données personnelles mises en œuvre au sein de l'association.

C) Les cibles du R.G.P.D.

Les cibles prioritaires de ce nouveau règlement sont clairement les entreprises qui collectent les données personnelles, parfois très sensibles, à des fins commerciales.

Une association sportive locale et sa liste d'adhérents avec nom, prénom, adresse, et taille n'est manifestement pas « dans le collimateur » direct de la Commission Européenne, mais un règlement européen est, comme rappelé ci-dessus, obligatoire, de portée générale et immédiatement applicable dans les Etats membres de l'Union Européenne et, à ce titre, chacun doit, dans notre pays, s'y conformer. Le règlement indique d'ailleurs, d'une manière générale, qu'il concerne « toutes les structures » qui rassemblent ce qu'on appelle des données personnelles.

L'application du R.G.P.D., le 25 mai 2018, est donc l'occasion pour chaque organisation de faire un état des lieux des données personnelles qu'elle collecte sur ses bénévoles, ses adhérents ou ses employés.

Ensuite, il faudra s'assurer que le traitement de ces données et les outils utilisés respectent bien les nouvelles dispositions en vigueur.

D) Êtes-vous concernés ?

- Oui, si vous avez un fichier des membres de votre association et que vous stockez leurs données personnelles (date de naissance, adresse mail, etc. ...)
- Oui, si vous avez un fichier de contacts à qui vous envoyez des e-mails/newsletters.
- Oui, si vous avez des salariés et que vous stockez leurs données personnelles.

E) Les dispositions du R.G.P.D.

- S'assurer que l'individu ait donné son consentement, libre et éclairé, pour faire partie de votre fichier : c'est-à-dire qu'il doit être en mesure de savoir quelles informations vous stockez à son sujet et quel en est votre usage.
- Justifier la raison pour laquelle vous stockez ces données.
- Prévoir la possibilité pour l'individu de demander la suppression de ses données personnelles au moins aussi facilement qu'il a donné son consentement (droit à l'oubli).
- Concevoir des conditions particulières pour le traitement des données des enfants. La réglementation européenne comporte des dispositions spécifiques pour les mineurs de moins de 16 ans. L'information sur le traitement des données les concernant doit être rédigée en des termes clairs et simples, que le mineur peut aisément comprendre. Le consentement doit être recueilli auprès du titulaire de l'autorité parentale. Les États membres de l'Union Européenne peuvent abaisser cet âge, prévu par la loi, sans qu'il puisse être inférieur à 13 ans. Devenu adulte, le consentement donné sur un traitement doit pouvoir être retiré et les données effacées.

F) De quel type de données parle-t-on pour une association professionnelle ?

Les associations devront tenir un registre complet de toutes les activités de traitement des données personnelles. À titre d'exemple, voici les informations que doit contenir ce registre pour une liste de membres d'une association.

- Finalité du traitement : Paiement de la cotisation annuelle, envoi d'informations concernant la profession (événement, bourse de recherche, évolution de la réglementation, campagnes d'information, etc.), étude des profils des membres pour pouvoir mieux cibler le recrutement de nouveaux membres, remboursement des frais de transports pour les réunions organisées par l'association (comité scientifique, réunion du bureau, etc.).
- Catégories de données personnelles concernées : Données d'identification (civilité, titre, nom, prénom, sexe, adresse, e-mail, téléphone, fonction, etc.), informations d'ordre économique et financière (date de paiement, moyen de paiement, banque émettrice du chèque, IBAN), données de connexion (login, mot de passe).
- Catégories de personnes concernées : Membres de l'association.
- Les destinataires : Membres de l'association.

Le R.G.P.D. prévoit une méthodologie de mise en conformité avec le dispositif en 6 étapes. Elle est éditée sur le site de la CNIL, je vous la transmets en pièce jointe du présent e-mail.

Nous espérons que l'application, au sein de votre structure, de cette méthodologie, vous donnera l'occasion d'auditer vos pratiques, de mieux comprendre les données collectées jusqu'alors, de vous questionner sur la pertinence de leur collecte et de prendre de bonnes résolutions en mettant de l'ordre en 2018 dans vos fichiers contenant des données personnelles.

Veillez recevoir, Madame la Présidente, Monsieur le Président, nos salutations sportives les meilleures,