LE REGLEMENT EUROPEEN SUR LA PROTECTION DES DONNEES

Sources : CNIL, CNOSF, Jurisassociations

Depuis plusieurs mois, le « RGPD » est agité par la vague médiatique comme un épouvantail.
Pourtant, depuis 40 ans, la loi dite « Informatique et libertés » encadre très strictement en France la collecte et l'exploitation des données personnelles.

Loin d'être une révolution, le nouveau Règlement européen *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* (ci-après « RGPD »), applicable dans tous les Etats membres de l'Union européenne depuis le 25 mai 2018, comprend néanmoins de réelles évolutions.

La présente fiche présente les points-clés pour mettre votre structure (ligue, comité, club) en conformité avec la nouvelle réglementation.

DEFINITIONS

L'article 4 du RGPD définit à la fois :

- les « données à caractère personnel » : « *toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée personne physique identifiable une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* »,
- le « traitement » de ces données : « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou ensemble de données à caractère personnel telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* ».

En résumé, toute gestion de salariés, de bénévoles, de membres d'une association, de mécènes, ou de clients, constitue un traitement de données personnelles, à travers leur nom, n° de licence ou de client, pseudo, adresse IP, badgeuse, etc.
Le fait que le traitement soit manuel et sans système informatique n'y change rien.

Le même article 4 définit également :

- le « responsable du traitement » : est ainsi désigné « *la personne, physique ou morale, l'autorité publique, le service ou autre organisme, qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* »,
- le « sous-traitant » : « *la personne, physique ou morale, l'autorité publique, le service ou autre organisme, qui traite les données personnelles pour le compte du responsable du traitement* ».

La fédération, une ligue, un comité et un club sportif sont donc, chacun à leur niveau, responsable du traitement des données personnelles de leurs salariés, de leurs adhérents, de leurs bénévoles ou des acheteurs de leurs produits ou billets.
Les hébergeurs de sites internet, les routeurs de mailing, les prestataires de billetterie ou de CRM, les fournisseurs de boutique en ligne, les solutions Cloud etc, auxquels une ligue, un comité ou un club sportif recourent, sont considérés comme leurs sous-traitants et partagent avec eux une coresponsabilité quant au respect du RGPD.

Focus : données des licenciés fédéraux

Nous avons mis à jour les conditions générales d'adhésion à la FFHandball pour 2018-19 à l'aune du RGPD. 3 principes à retenir :
- seule la fédération est propriétaire de la base de données des licenciés ; toute utilisation par une ligue, un comité ou un club doit OBLIGATOIREMENT recueillir l'accord préalable de la fédération,
- pour les communications électroniques de la fédération, d'une ligue ou d'un comité, relatives à leurs activités Handball, le consentement du licencié est donné au moment de son adhésion à la fédération,
- pour toute communication par ou pour un tiers (partenaire etc), seuls les licenciés ayant donné leur accord sur la case spécifique prévue à cet effet, pourront être sollicités.

PRINCIPES

Dans une volonté d'harmonisation au sein de tous les Etats européens, le RGPD renverse l'approche qui prévalait jusque-là en France :

Avant	Après
Formalités préalables à effectuer auprès de la CNIL (déclaration ou autorisation, selon la nature du traitement)	- Responsabilité des acteurs - Contrôle a posteriori (en France par la CNIL)

Il est donc désormais nécessaire non seulement de respecter les exigences de la réglementation, mais également de pouvoir démontrer ce respect et les mesures mises en œuvre pour le garantir.

3 principes centraux

1. Les données personnelles doivent être :
   - exactes (donc mises à jour si nécessaire),
   - pertinentes et limitées à la finalité de leur utilisation,
   - traitées de manière loyale et transparente,
   - sécurisées.

Toute personne doit ainsi pouvoir :
- connaitre précisément les objectifs pour lesquels ses données personnelles sont collectées,
- accéder aux données qui la concernent et, le cas échéant, les faire modifier,
- s'opposer, à tout moment, à leur utilisation (par exemple en se désinscrivant d'une newsletter),
- les faire effacer lorsqu'elles ne sont plus nécessaires aux finalités du traitement ou lorsqu'elles ont fait l'objet d'un traitement illicite.

2. Le traitement doit être consenti : la personne concernée doit avoir manifesté sa volonté par un acte positif clair, libre et spécifique.

C'est le système d'opt-in qui doit être utilisé : la case de consentement ne peut pas être pré-cochée et c'est la personne elle-même qui doit la cocher pour formaliser son accord.
Dans ce cadre, il est essentiel que la procédure de prise de licence soit réalisée par l'individu lui-même et non pas son club, car les conditions générales d'adhésion à la FFHandball doivent être acceptées (en cochant la case prévue à cet effet) par le licencié et lui seul – ou son représentant légal si le licencié est mineur.

3. En cas de faille de sécurité et/ou de violation importante des données personnelles, le responsable du traitement doit informer les personnes concernées et la CNIL.

La CNIL doit être informée dans les 72 heures si la violation est susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.
Pour les personnes elles-mêmes, c'est la nature de la violation (par exemple : un chiffrement rend-il inexploitable les données accidentellement dévoilées ?) qui guidera le choix de les informer. Dans tous les cas, nous conseillons de répondre si des personnes vous interrogent.

MISE EN CONFORMITE

Nous recommandons de procéder par étapes successives :

1. Désignez un référent unique pour toutes les questions liées à la protection des données (au niveau fédéral, ce référent sera le « Délégué à la protection des données » dont la désignation est obligatoire),

2. Recensez et cartographiez les traitements existant dans votre structure (finalité, types de données, personnes concernées et destinataires, sous-traitants éventuels, durée de conservation, mode de sécurisation),

3. Procédez à une analyse d'impact (évaluer le niveau de risque sur les droits et libertés des personnes, en cas de violation),

4. Tenez un registre écrit des traitements mis en œuvre (identification du pilote de chaque traitement, catégories de données traitées, objectifs, acteurs –internes et/ou externes- ayant accès aux données et les traitant, circuit des flux de données, durée de conservation, mesures de sécurité technique et organisationnelle),

5. Mettez à jour les mentions légales sur vos différents supports (cookies sur le site internet, bon de commande, formulaire de contact en ligne) et concluez les avenants nécessaires aux contrats avec vos sous-traitants,

6. Informez vos salariés, bénévoles, adhérents des actions mises en œuvre pour vous conformer au RGPD.

SANCTIONS

Deux types de sanctions existent :

Administratives (prononcées par la CNIL)	**Pénales (articles 226-16 et suivants du code pénal)**
Avertissement ou mise en demeure du responsable du traitement	300.000 € d'amende et 5 ans d'emprisonnement, notamment en cas de : - non-respect de l'obligation de sécurité - détournement de la finalité des données personnelles
Limitation ou suspension d'un traitement	1.500 € d'amende par infraction constatée, notamment en cas de : - absence d'information des personnes concernées - non-respect des droits des personnes (consentement, accès, rectification etc)
Ordre d'effacer, rectifier ou limiter des données	
Ordre de satisfaire aux demandes des personnes (accès, rectification etc)	
Jusqu'à 20 M€ (ou 4% du chiffre d'affaires annuel mondial)	

Aller plus loin :

Site de la CNIL (www.cnil.fr) : **TOUTES les informations utiles** pour vous accompagner (par où commencer ? se préparer, passer à l'action, bons réflexes, boite à outils, etc).