FFESSM

IMMERSION & EMOTION

Le RGPD

CDN du 1 juin 2018

Le RGPD

Approuvé par 29 pays européens signataires, tous les établissements qui traitent des données personnelles doivent s'y conformer. **Le règlement est entré en application le 25 mai 2018.**

Le RGPD restitue par le droit, le pouvoir aux individus sur leurs données personnelles, un signal fort envoyé notamment aux GAFA (Google, Amazon, Facebook, Apple).

C'est quoi une donnée personnelle ?

Une personne est identifiée lorsque son nom apparaît dans un fichier associé à des données qui lui sont propre comme :
Immatriculation | Localisation | Adresse électronique [Date de naissance [Infos de paiement | Numéro de téléphone …

Identifier les données sensibles qui font l'objet de dispositions particulières :
Données génétiques ou biométriques | Données médicales | Sanctions administratives ou suspicions | Opinions politiques | Orientations sexuelles.

11 obligations dont : droit à une obligation complète, droit d'être informé en cas de violation de données, droit à l'oubli, droit à la limitation du traitement, droit à la portabilité, droit d'opposition, droit spécifiques pour les mineurs.

Le RGDP

Qui est responsable devant la loi ?

- Le Responsable de traitement :
Toute personne physique, morale, le service ou un autre organisme, **qui détermine les finalités et les moyens** du traitement de données à caractère personnel.

- Le **Sous-traitant (ST)** :

Toute personne physique, morale, service ou un autre organisme, **qui traite des données** à caractère personnel **pour le compte d'un responsable de traitement**.
- les prestataires de services informatiques (hébergement, maintenance, intégrateur, sécurité…)

La loi introduit des sanctions :

Des amendes pouvant atteindre **20 M€ ou 4%** du chiffre d'affaires global de l'organisation

Autorité de contrôle

En France, c'est la CNIL qui est chargé de contrôler et faire appliquer le règlement.
Missions :
Informer et protéger les personnes
Accompagner et conseiller les professionnels
Contrôler et sanctionner

Droits des personnes

- Information
- Consentement
- Accès
- Modification
- Opposition
- Plainte (auprès de la CNIL)
- Portabilité
- Droit à l'oubli (dans la limite du cadre de la loi…)

Articles spécifiques

- Droit à la limitation du traitement (la personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement dans certains cas)
- Droit à ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé
- Communication à la personne concernée d'une violation de données personnelles

Calendrier : c'était le 25 mai !

Une phase progressive de mise en conformité sans sanction les premiers mois d'entrée en application du règlement est accordée par la CNIL

Il faut démontrer que les étapes de mise en conformité préconisées par la CNIL ont été engagées.

Le RGDP

Etapes de mise en conformité

- Désigner un responsable de la mise en conformité (ou DPO selon les cas)
- Cartographier les traitements
- Analyser les écarts avec le règlement
- Plan d'action de mise en conformité
- Organisation et documentation des processus internes : registre

Données "clients" :

Fichiers clients (CRM),
Outils Métiers (site web), Mailing, Réseaux sociaux,
… en interne comme en externe (sous traitants, tiers etc.)

Données "salariés" :

CV, dossiers professionnels, organigramme, planning, outils métiers,
gestion de terminaux, vidéosurveillance, badge, tracking GPS…

Plan d'actions

- **Documenter** sa conformité via registre, audit, études, traces…
- **Fin des déclarations CNIL**
- **Co-responsabilité des prestataires** et sous-traitants (conformité RGPD à mettre dans les contrats)
- **Cybersécurité** : Mettre en oeuvre des moyens adaptés et notifier des failles de sécurité sous 72h à la CNIL + users
- **Renforcement des droits des personnes :** Information et consentement, portabilité, droit à l'oubli etc...

Le RGDP pour les associations sportives

Les associations sportives sont bien soumises au RGPD

Recommandations

- **Désigner un responsable conformité au RGPD** (pas obligatoire pour les clubs, mais conseillé)
- **Identifier les données personnelles collectées** (Eviter de collecter des données sensibles)
- **Rédigez un état des lieux et un plan d'action**
- **Informez les adhérents, gestionnaires, salariés**
- **Conservez les documents nécessaires** (registre non obligatoire, uniquement pour Ets > 250 salariés
- **S'assurer de la sécurité des données et de l'existence d'une procédure en cas de fuite et de la portabilité des données**

Rédiger un état des lieux

- Préciser ce que vous faites de ces données personnelles (quel "traitement" au sens du règlement)
- **Préciser vos objectifs** du traitement de données (connaître vos membres, leur offrir des formations…)
- Préciser vos systèmes: vérifiez que votre fournisseur maîtrise le RGPD. Où les données sont stockées? qui y a accès? quelle est la sécurité?

Rédiger vos mentions légales (site) avec notamment les informations suivantes:

- l'identité et les coordonnées du responsable du traitement ou son représentant
- les finalités du traitement;
- si les données sont transférées vers un destinataire dans un pays tiers
- la durée pendant laquelle les données à caractère personnel seront conservées
- l'existence du droit de demander l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement ainsi que du droit de s'opposer au traitement et du droit à la portabilité des données
- le droit d'introduire une réclamation

Le RGDP

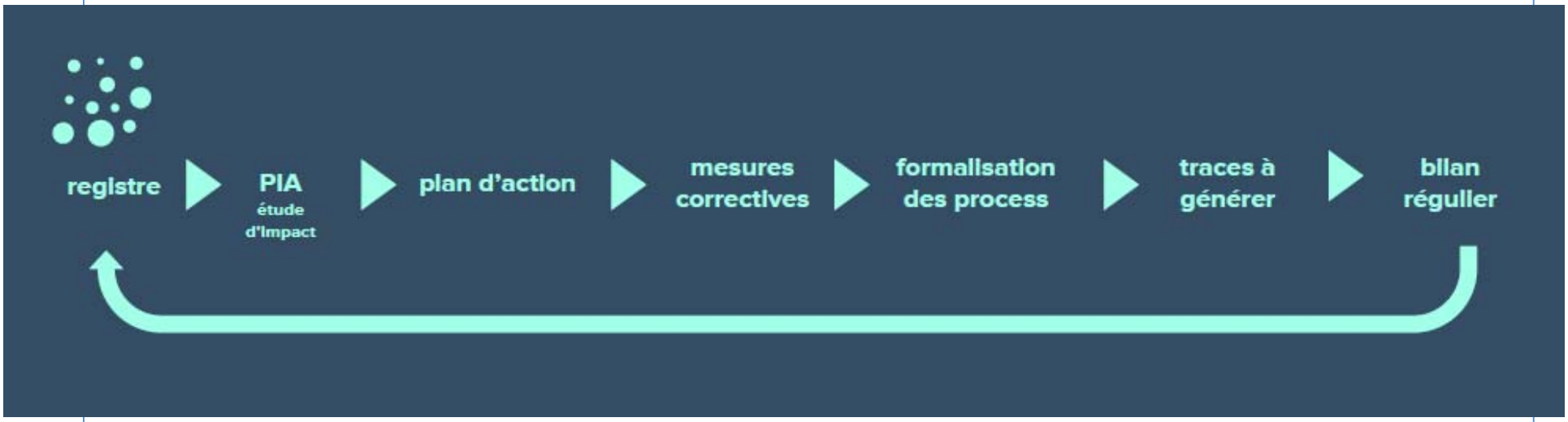
- Assurez vous de l'obtention du consentement explicite de vos membres ou adhérents et qu'ils comprennent pourquoi ces données sont collectées. Concrètement votre contrat d'adhésion devra comporter des mentions relatives aux données personnelles. Même votre formulaire de contact en ligne devra comporter des mentions (renvoie vers les mentions légales par exemple). Attention, vous devrez être en mesure de prouver le recueil de ce consentement le cas échéant (en cas de contrôle de la CNIL).

- Rappelez-vous que vos membres peuvent retirer leur consentement à tout moment dès qu'ils le demande. Donc votre système de gestion devra permettre la modification ou la possibilité d'effacer les données si cela vous est demandé.

- Si vous possédez un système existant, **vérifiez que votre fournisseur actuel maîtrise GDPR et ses implications**.

- **Assurez-vous de la sécurité des données**. Ou sont-elles stockées? par qui? qui y a accès?

Le RGDP



En Conclusion :
Se conformer parfaitement à la loi sera certainement compliqué pour un club, par contre mettre en place les bons outils permettant de prouver sa bonne foi est assez simple. Sachant qu'une partie des obligations du responsable des traitements peut être déléguée à son sous-traitant du moment que celui-ci est bien au fait des règles de la RGPD et de la mise en place des moyens adéquats, prouver que l'on a fait les efforts nécessaires pour se mettre en conformité, devient accessible à tous.

Documentation

- Site de la CNIL : https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes
- Site de l'ANSSI : http://www.ssi.gouv.fr/entreprise/precautions-elementaires/dix-regles-de-base/
- Document PDF CNIL "se préparer en 6 étapes" : https://www.cnil.fr/sites/default/files/atoms/files/pdf_6_etapes_interactifv2.pdf
- Modèle de registre : https://www.cnil.fr/sites/default/files/atoms/files/registre-reglement-publie.xlsx