Le service juridique n'a eu aucune formation spécifique en ce domaine mais ce document se veut informatif.
En cas de questions vous pouvez aussi poser des questions à la CNIL : coordonnées ci-dessous…

Le règlement (Union européenne) n°2016/679 dit règlement général sur la protection des données (RGPD) renforce la protection des personnes concernées par un traitement de leurs données à caractère personnel et harmonise le droit Européen en la matière.

Les dispositions du RGPD sont applicables à compter du **25 mai 2018**.

Depuis plusieurs mois, la CNIL a édité et élaboré des articles sur le RGPD…

Nous vous avons fait part de ces supports à travers divers supports tels que la revue de presse, le Bulletin d'infos, le Flash Info (n°09-2018), la dernière revue Info Conso *2018-01* (p. 15).

Voir de plus amples informations sur le sujet :

- **Les Associations sont-elles concernées par le RGPD ?**

Ce règlement donne des droits aux particuliers mais en tant qu'associations, elles aussi doivent se conformer au RGPD si elles collectent et stockent des données personnelles.

Lien CNIL : https://www.cnil.fr/cnil-direct/question/1327?visiteur=pro

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

Selon la loi Art. 2 de la loi "Informatique et libertés"
« **Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement** »

Une personne est identifiée lorsque par exemple, son nom apparaît dans un fichier.

Cela peut désigner : un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal,…

Peu importe que ces informations soient confidentielles ou publiques.

A noter : pour que ces données ne soient plus considérées comme

personnelles, elles doivent être rendues anonymes de manière à rendre impossible toute identification de la personne concernée : noms masqués, visages floutés, etc.

Attention : s'il est possible par recoupement de plusieurs informations (âge, sexe, ville, diplôme, etc.) ou par l'utilisation de moyens techniques divers, d'identifier une personne, les données sont toujours considérées comme personnelles.

Nos associations suivant leurs activités peuvent collecter différentes données selon leurs activités et leur durée de conservation peut varier selon leur nature : collecte de données pour les adhésions, pour l'UNAF, pour la DGCCRF, pour la comptabilité, … et selon les obligations légales qui y sont rattachées.

- **Doit-on désigner un délégué à la protection des données ou DPO** ?

Le DPO est obligatoire dans 2 cas :

- Pour les organismes publics ;
- Vous êtes une entreprise dont l'activité de base vous amène à réaliser un suivi régulier et systématique des personnes à grande échelle, ou à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

  Il n'est donc pas obligatoire dans nos structures.
  Cependant cette désignation est tout de même possible.

  Au-delà de ce DPO, il faut désigner un référant qui gérera le traitement de ces données et traitera les demandes d'opposition, de rectification qui peuvent émaner des adhérents ou des autres personnes auprès desquelles on a collecté des données.

- **Les étapes pour s'y conformer**…

  La CNIL a élaboré un document dans ce sens en insistant sur 4 étapes à respecter…

Lire avec attention ces différentes étapes :
https://www.cnil.fr/fr/rgpd-par-ou-commencer

1/ Le registre : La CNIL conseille d'élaborer un registre sur les données qui sont collectées.
Ce registre n'est obligatoire que pour les grosses structures de 250 salariés et ne concerne donc pas nos associations mais il est tout de même utile d'en élaborer un.

La CNIL a élaboré **plusieurs types de registres** qui sont sous plusieurs formes (Word, Excel, PDF, Rtf) :

https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf

https://www.cnil.fr/fr/rgpd-et-tpepme-un-nouveau-modele-de-registre-plus-simple-et-plus-didactique

Pour chaque activité recensée, vous devrez créer et tenir à jour une fiche de registre.

2/ Le tri des données :
Le but de ce tri est d'identifier les données qui sont utiles lors de cette collecte et d'identifier si ces données sont qualifiées de « sensibles » ce qui correspond à des informations d'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes.

Pour faciliter le tri des données et la création du registre, la CNIL conseille de réaliser une cartographie afin de pouvoir créer le registre plus facilement.

Lien pour faire cette cartographie : https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles

3/ Respect des données personnelles : lors de cette étape, il convient d'informer du traitement des données par le biais du site internet de l'association, lors de la transmission du bulletin d'adhésion.

Lors de l'adhésion d'un adhérent : il faut transmettre un document qui pourra être adossé ou indiqué sur le bulletin.

Exemple de document à personnaliser :
https://www.cnil.fr/fr/modele/mention/formulaire-de-collecte-de-donnees-personnelles

Sur les sites des associations :
Informer sur la finalité des collectes des données (transmission à divers acteurs UNAF, DGCCRF, services de l'association, ANCV,…), sur la durée de conservation des données, demander aux adhérents leurs accords dans la transmission de leurs données par le biais d'une case à cocher ou d'une signature prouvant cette accord (**un consentement implicite n'est pas valable**), prévenir de la possibilité da faire opposition.

Durée de conversation des données ?
https://www.cnil.fr/cnil-direct/question/499?visiteur=pro

Si la loi n'impose pas une durée légale, voir combien de temps cette conservation est utile ;

Quelques durées légales :
Comptabilité : 10 ans
Gestion du personnel : bulletin de paye, registre : 5 ans
Dossier juridique : 5 ans à compter de sa clôture

Lien

Avec le RGPD, les droits des personnes à qui on collecte des données sont renforcés : ces droits regroupent le droit d'accès à ces données, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation du traitement selon ce qui est utile.

Définitions sur le droit d'accès, de rectification, d'opposition :
https://www.cnil.fr/cnil-direct/question/512

Dans ce contexte, les adhérents doivent pouvoir contacter le responsable des données de la structure assez rapidement par d'un numéro de téléphone dédié, d'une messagerie spéciale.

Quel est le délai raisonnable pour traiter des données personnelles en cas de demande d'un adhérent?

On considère que le délai d'un mois est raisonnable.

4/ La sécurité des données :

Il faut s'assurer que le fichier et les mails soient bien sécurisés : mots de passe suffisants, …

- **Pour aller plus loin :**

Voici plusieurs documents ou modules sur le sujet :

- Module sur *Fun mooc* du CNAM avec la collaboration du personnel de la CNIL : https://www.fun-mooc.fr/courses/course-v1:CNAM+01032+session01/about

- Module d'un You tubeur dénommé *Cookie élaboré avec la CNIL* : https://www.youtube.com/watch?v=OUMGp3HHel4

- Un *guide sur la RGPD élaboré par la CNIL* pour aider les PME : https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-guide-rgpd-tpe-pme.pdf

- J'estime ne pas être en conformité avec le RGPD à la date du 25 mai 2018, est-ce que j'encours des sanctions de la part de la CNIL ?

Les associations ne sont pas la cible principale de cette réglementation mais elles sont tout de même susceptibles d'être contrôlées.
La loi prévoit des sanctions administratives (2à 4% du chiffre d'affaire pour une entreprise et 10 à 20 millions d'euros d'amende) puis pénales sont prévues en cas d'irrespect du RGPD.

- **Alertes de la CNIL :**

Attention, depuis plusieurs mois des personnes malveillantes insistent sur les sanctions que peuvent encourir les entités en cas de non respect au RGPD.
Des nouvelles arnaques sont alors entrain de se mettent en place avec le RGPD…
Ce type d'arnaque prend actuellement plusieurs formes :

- Des individus ont proposés des ***services « clefs en mains » à des tarifs excessifs*** ;
- Des mails frauduleux ou appels surtaxés dans le but de respecter le RGPD peuvent aussi toucher les structures.

Pour éviter ce genre de déconvenues, n'hésiter pas à contacter la CNIL et ne répondez pas à ce type d'appels ou de mails douteux.

- **Le numéro de la CNIL :** 01 53 73 22 22
- **Site de la CNIL :** www.cnil.fr
- **Page de contact de la CNIL : https://www.cnil.fr/webform/nous-contacter**