POUR LES ASSOCIATIONS
LE DÉPARTEMENT AGIT !

SAÔNE & LOIRE DÉPARTEMENT

GESTION ADMINISTRATIVE ET FINANCIÈRE

LA PROTECTION DES DONNÉES ET LE RGPD

BONNES PRATIQUES

Le Règlement général des données personnelles (RGPD) s'applique à tout organisme traitant des données personnelles* comme les associations. Les dirigeants doivent s'assurer d'un traitement sécurisé des données.

LES BONNES PRATIQUES EN MATIÈRE DE PROTECTION DES DONNÉES PERSONNELLES

Il est nécessaire de se poser les bonnes questions. Une réunion animée par le secrétaire de l'association peut permettre de s'interroger sur les questions suivantes :

- Quelle est la finalité (l'objectif) de la collecte de données ?
  - L'objectif doit être déterminé et légitime, et ne pas être contraire au droit.
- De quelles données ai-je réellement besoin pour atteindre cet objectif ?
  - Données pertinentes et nécessaires.
- Qui pourra (aura besoin) d'accéder à ces données dans l'association en fonction de ses missions ?
  - Les données doivent être consultées et utilisées par le moins de personnes possible.
- Combien de temps sera-t-il nécessaire de les conserver ?
  - Déterminer une durée en fonction de l'objectif de la collecte.
- Comment les personnes seront-elles informées de l'usage qui sera fait de leurs données ?
  - Être transparent sur l'utilisation de leurs données et permettre aux membres de choisir les informations qu'ils souhaitent recevoir (publicité, partenaires, fédération…).
- Comment pourront-elles exercer leurs différents droits (droit d'accès, droit de rectification…) ?
  - Expliquer aux adhérents qu'ils peuvent demander une rectification ou l'effacement de certaines de leurs données.

LES ÉTAPES À RESPECTER POUR METTRE MON ASSOCIATION EN CONFORMITÉ

1- **Recensez** les fichiers contenant des données personnelles au sein d'un **registre numérique ou papier**. Dans ce registre, vous devez créer une fiche par activité (ex : adhésions) en précisant les détails du traitement (finalité, données collectées, personnes concernées, destinataires, durées de conservation, mesures de sécurité…).
2- **Faites le tri** dans vos données, en supprimant les données qui ne sont pas nécessaires à l'activité de votre association (par ex : les fichiers d'anciens membres).
3- **Faites preuve de transparence**, en informant les adhérents à chaque fois que des données personnelles sont recueillies, sous format papier ou numérique (bulletins d'adhésion, questionnaires…). L'information des adhérents doit être faite par le biais d'une mention d'informations à l'oral ou par le biais d'une affiche. **Toute forme d'information est conseillée**.
4- **Facilitez l'exercice des droits** des personnes : droit **d'obtenir une copie** des données les concernant, droit de **rectifier** les informations inexactes ou incomplètes, droit de **faire effacer** les données si elles ne sont plus utiles, droit de **s'opposer** au traitement de ses données pour des raisons particulières (sauf si le traitement repose sur une obligation légale).
5- **Sécuriser les données** pour **limiter les risques d'accès illégitime aux données**, de disparition des données ou de modification non désirée.

*Voir la fiche **La protection des données personnelles pour les associations**

S'ASSURER DE LA SÉCURITÉ ET DE LA CONFIDENTIALITÉ DES DONNÉES

- Fermeture à clé des locaux, armoires, bureau
- Définir qui pourra disposer des habilitations pour accéder à ces informations pendant la durée du mandat
- Mots de passe individuels suffisamment complexes, renouvelés régulièrement
- Suppression des comptes utilisateurs en cas de départ
- Sécurisation des postes de travail (ex : verrouillage automatique de session, antivirus et logiciels à jour)
- Procédures de sauvegardes régulières et de récupération des données en cas d'incident
- Pour l'envoi de mail, mettre les destinataires en copie cachée
- Pour les groupes WhatsApp : supprimer les anciens membres
- Signature d'une charte informatique pour les membres de l'association (exemple : qui rappelle les bonnes pratiques et consignes de sécurité pour les personnes chargées de collecter les données)

QUE FAIRE EN CAS DE VIOLATION DE DONNÉES ?

Lorsque des données personnelles ont été, de manière accidentelle ou malveillante, détruites, perdues, modifiées ou divulguées, il s'agit d'une « violation de données ».
Si un tel incident se produit, il est nécessaire de le documenter au sein de l'association. En cas de contrôle, ce document est vérifié par les services de la CNIL.
En cas de risque pour les personnes concernées par l'incident, vous devez signaler cette violation à la CNIL dans les 72 heures, via leur site web.

CAS PARTICULIER :
La collecte des données sensibles pour les associations.

Voir la fiche **La protection des données personnelles pour les associations**

POUR EN SAVOIR PLUS sur ces notions, consultez la fiche
« La protection des données personnelles pour les associations »