



LE RGPD EN PRATIQUE POUR LES ASSOCIATIONS

Le nouveau Règlement Général sur la Protection des Données Personnelles (RGPD) est entré en vigueur le 25 mai dernier. Voici un mémo pour accompagner les associations dans leur mise en conformité.

Qui est concerné ?

Le Règlement européen sur la protection des données personnelles concerne **toutes les structures qui rassemblent ce qu'on appelle des "données personnelles"**, c'est-à-dire « toute information se rapportant à une personne physique identifiée ou identifiable [...] directement ou indirectement ». A partir du moment où une association collecte des informations sur ses membres (par exemple : le nom, le prénom, l'adresse e-mail, l'adresse postale, le numéro de téléphone ...) , elle doit **avoir entrepris les actions nécessaires à la mise en conformité de votre base de données.**

Que veut dire « mise en conformité » ?

La mise en conformité RGPD est essentiellement organisationnelle : elle correspond à la mise en place d'outils et de bonnes pratiques au sein de votre association. Plusieurs actions peuvent être recommandées.

Les actions principales à mener

- **Action 1** : Désigner un pilote au sein de son association
- **Action 2** : Recenser ses fichiers dans un registre vous permettant d'avoir une vision d'ensemble de votre traitement de données. Les associations peuvent s'appuyer sur le modèle de registre proposé par la CNIL sur son site internet [à télécharger ici](#)
- **Action 3** : faire le tri dans ses données. Pour chaque fiche de registre créée, il convient de vérifier
 - que les données traitées sont nécessaires à ses activités
 - qu'aucune donnée dite « sensible » n'est traitée, ou, si c'est le cas, que l'association a bien le droit de les traiter ;
 - que seules les personnes habilitées ont accès aux données dont elles ont besoin
 - que les données ne sont pas conservées au-delà de ce qui est nécessaire.
- **Action 4** : Respecter les droits des personnes. À chaque collecte de données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information comportant notamment les éléments suivants :
 - « la finalité » ; par exemple pour gérer l'achat en ligne du consommateur) ;
 - le « fondement juridique » : il peut s'agir du consentement de la personne concernée, de l'exécution d'un contrat, du respect d'une obligation légale qui s'impose à vous, de votre « intérêt légitime ») ;
 - qui a accès aux données (indiquez des catégories : les services internes compétents, un prestataire, etc.) ;
 - combien de temps ces données sont conservées
 - les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits (via leur espace personnel sur votre site internet, par un message sur une adresse email dédiée, par un courrier postal à un service identifié) ;
 - si l'association transfère les données hors de l'Union européenne (précisez le pays et l'encadrement juridique qui maintient le niveau de protection des données).

Des exemples de mentions sont disponibles sur le site internet de la CNIL, [à consulter ici](#).

- Action 5 : sécuriser les données

Cela veut dire minimiser les risques de pertes de données ou de piratage. Les mesures à prendre, informatiques ou physiques, dépendent de la sensibilité des données traitées et des risques qui pèsent sur les personnes en cas d'incident : mises à jour de vos antivirus et logiciels, changement régulier des mots de passe et utilisation de mots de passe complexes, ou chiffrement de vos données dans certaines situations.

Le mouvement associatif a sur le sujet sorti une note assez complète : [FAQ Associations et RGPD](#)

En cas de contrôle, une association doit être en mesure de **présenter un plan d'action et montrer les premières étapes** mises en place pour être en conformité. Comme indiqué sur le site Internet de la CNIL, « *les contrôles opérés auront essentiellement pour but, dans un premier temps, d'accompagner les organismes vers une bonne compréhension et la mise en œuvre opérationnelle des textes. En présence d'organismes de bonne foi, engagés dans une démarche de conformité et faisant preuve de coopération avec la CNIL, ces contrôles n'auront normalement pas vocation à déboucher, dans les premiers mois, sur des procédures de sanction sur ces points.* ».

En cas d'infraction au RGPD, des **sanctions lourdes** (jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire mondiale d'une organisation) pourront être appliquées.

Pour en savoir plus Consultez le [guide en 6 étapes élaboré par la CNIL](#)

RGPD : se préparer en 6 étapes

Le 25 mai 2018, le règlement européen est entré en application. De nombreuses formalités auprès de la CNIL disparaissent. En contrepartie, la responsabilité des organismes est renforcée. Ils doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

Etape 1

Désigner un pilote

Désigner un pilote

Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données. En attendant 2018, vous pouvez d'ores et déjà désigner un « correspondant informatique et libertés », qui vous donnera un temps d'avance et vous permettra d'organiser les actions à mener.

> [En savoir plus](#)

Etape 2

Cartographier

Cartographier vos traitements de données personnelles

Pour mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez, commencez par recenser de façon précise vos traitements de données personnelles. L'élaboration d'un registre des traitements vous permet de faire le point.

> [En savoir plus](#)

Etape 3

Prioriser

Prioriser les actions à mener

Sur la base de votre registre, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

> [En savoir plus](#)

Etape 5

Gérer les risques

Gérer les risques

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact relative à la protection des données (AIPD).

> [En savoir plus](#)

Etape 6

Organiser

Organiser les processus internes

Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire).

> [En savoir plus](#)

Etape 5

Documenter

Documenter la conformité

Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

> [En savoir plus](#)

5 POINTS POUR ÊTRE CONFORME AU

RGPD



AU SEIN DE L'ORGANISATION

- Désigner un DPO (délégué à la protection des données obligatoire dans certains cas).
- Tenir un registre numérique des traitements des données personnelles.



SUR VOTRE SITE INTERNET

- Créer un espace où chaque membre pourra supprimer, modifier et consulter ses données.
- Modifier vos CGV/CGU et mentions légales.
- Conserver uniquement les données nécessaires au regard des besoins.



AU NIVEAU DU CONSENTEMENT

- Afficher clairement la demande de consentement dans vos CGV/CGU.
- Donner la permission à chaque membre de pouvoir retirer son consentement facilement.
- Conserver les approbations de consentement.



DANS VOS FORMULAIRES

- Informer les visiteurs de la façon dont leurs données sont et seront utilisées avant la demande de consentement.
- Insérer clairement vos demandes de consentement dans vos formulaires.
- Ajouter une case à cocher pour approuver le consentement.



DANS VOS NEWSLETTERS

- Informer les personnes contactées des conditions de traitement de leurs données.
- Intégrer un lien de désinscription permettant à vos destinataires de s'opposer à l'utilisation de leurs e-mails.
- Ajouter un lien permettant à vos utilisateurs de consulter/modifier/supprimer leurs données à tout moment.