Les obligations d’une association avec le RGPD

Description

Le Règlement Général sur la Protection des Données (RGPD) entré en vigueur en 2018 a fait naître de nombreuses obligations pour les sociétés ainsi que pour certains organismes. Néanmoins, ce dernier s’applique également aux associations, qui doivent ainsi procéder à une mise en conformité au RGPD au même titre que ses entités voisines.

Obtenir un devis gratuit RGPD

Pourquoi les associations sont-elles concernées par le RGPD ?

Pour mieux comprendre l’étendue de l’application du RGPD, il convient dans un premier temps de voir quel **type d’association** est concernée par ce règlement, puis en quoi le traitement des données à caractère personnel est le seul **critère d’applicabilité** du règlement.

Un critère d’applicabilité unique : le traitement de données à caractère personnel

Le RGPD concerne tout **organisme public ou privé** traitant des données personnelles, pour son compte ou non, dès lors qu’il est établi sur le **territoire de l’Union européenne** ou que son activité cible directement des **résidents européens**.

Or, les associations sont régulièrement amenées à collecter de **nombreuses informations** dont des données à **caractère personnel** (*Exemple* : des informations sur ses adhérents). De ce fait, elle est également soumise à l’obligation de respecter les principes posés par le règlement.

A noter : On entend par donnée à caractère personnel toute information se rapportant directement ou indirectement à une personne physique identifiée ou identifiable au sens de l’article 4 du RGPD.

Les types d'associations concernées par le RGPD

Les associations, quel que soit leur type sont dans l'obligation de respecter la réglementation prévue par le RGPD dès lors qu'elles procèdent à la **collecte**, la **conservation** ou **l'utilisation** de données personnelles. Par conséquent, sont concernées par son application :

- Les associations loi 1901
- Les associations reconnues d'utilité publique
- Les associations de gestion agréée
- Les associations de fait

Bon à savoir : Le RGPD s'applique également au sous-traitant de l'association. Il s'agit de l'entreprise ou l'organisme qui va aider l'association dans le traitement des données personnelles.

Quels sont les grands principes à respecter par les associations soumises au RGPD ?

L'objectif du RGPD est de renforcer les droits des personnes en matière de **données personnelles**. Les associations sont soumises au respect de plusieurs grands principes et **leur responsabilité** peut être engagée dans certains cas.

Le respect des grands principes du RGPD

Pour répondre à son objectif de **renforcement des droits** des personnes, le RGPD a mis en place plusieurs **grands principes** à respecter qu'il convient de présenter :

- **La minimisation des données**: l'association doit limiter la collecte de données à celles strictement nécessaires à la finalité du traitement.
- **La licéité du traitement** : L'article 6-1 du RGPD liste six conditions dans lesquelles le traitement des données personnelles est permis. Si le traitement ne répond pas à au moins une des six conditions listées, il sera illicite.
- **La transparence** : l'association doit fournir plusieurs informations telles que : la finalité du traitement, la base juridique du traitement, ou encore la durée de conservation des données. De plus, ces informations doivent être accessibles aux personnes dont les données sont collectées.

Bon à savoir : Pour respecter l'obligation de transparence, l'association peut rédiger une politique de confidentialité RGPD

.

Les obligations du responsable de traitement

On entend par responsable de traitement, la personne **morale** ou **physique** déterminant **les finalités** et **moyens** d'un traitement. Il est notamment tenu de respecter le principe d'accountability consistant à mettre en œuvre des procédures et mécanismes internes permettant de démontrer le respect des règles liées à la protection des données.

A noter : En général, le responsable de traitement est une personne morale incarnée par son **représentant légal**.

L'association est un **responsable de traitement**, par conséquent elle est soumise au respect des obligations posées par l'article 5 du RGPD. Ainsi, elle doit mettre en place les mesures nécessaires à la garantie des **principes** posés par le RGPD :

- Le principe de privacy by default : une fois qu'un service a été communiqué au public, les standards de protection des données personnelles devront être appliqués par défaut.
- Le principe de privacy by design : l'association doit intégrer la protection des données à caractère personnel, et ce dès la conception de projets rattachés au traitement des données.

Comment procéder à la mise en conformité d'une association au RGPD ?

La mise en conformité au RGPD impose de mettre en œuvre un processus en vue d'atteindre un niveau de **protection des données personnelles** suffisant. Sur son site internet, le CNIL présente un processus comportant plusieurs actions à effectuer :

- Constituer un registre de traitement des données
- Faire le tri dans les données
- Respecter les droits des personnes
- Sécuriser les données personnelles

Constituer un registre de traitement des données

La constitution d'un **registre de traitement des données** permet d'avoir une vision d'ensemble sur ces derniers. Dans un premier temps, il faut identifier les **activités principales**

de l'entreprise ayant recours au traitement de données personnelles.

Il est pas la suite nécessaire de créer une ficher pour chaque activité recensée comportant les informations suivantes :

- L'objectif poursuivi
- Les catégories de données utilisées
- Les personnes ayant accès aux données
- La durée de conservation des données

Pour optimiser au mieux le registre, il faut maintenir un contact avec l'ensemble des personnes de l'entreprise susceptibles de traiter des **données personnelles**.

Bon à savoir : Il est recommandé de confier la tenue du registre au délégué à la protection des données (DPO). Ce dernier aura pour mission de le **mettre à jour** régulièrement.

Faire le tri dans les données

Les associations sont tenues de respecter le **principe de minimisation** des données posé par l'article 5-1 c). En effet, ce dernier dispose que les données à **caractère personnel** doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données)* ». Les données collectées doivent être **nécessaires** à la finalité du traitement.

Bon à savoir : On entend par **finalité de traitement**, l'objectif en vue duquel les données sont collectées ou exploitées par l'association. Cette dernière doit **impérativement** être définie par les associations.

Ainsi, lors de la collecte des informations, le **responsable de traitement** doit s'assurer que :

- Les données collectées sont nécessaires à l'activité de l'association
- Les données traitées ne sont pas « sensibles », auquel cas il faut s'assurer que l'association a bien le droit de les traiter
- Les données ne sont accessibles que par les personnes habilitées
- Les données ne doivent pas être conservées au-delà de la durée nécessaire

Respecter les droits des personnes

Les personnes dont l'association traite les données possèdent **des droits** qui leur ont

été accordés par le RGPD, à savoir :

- Un droit d'accès
- Un droit de rectification
- Un droit d'opposition
- Un droit d'effacement
- Un droit à la portabilité
- Un droit à la limitation du traitement

Il incombe au responsable de traitement de mettre en place **les mesures** veillant à respecter ces droits. De plus, il doit également veiller à recueillir le consentement de la personne concernée lors de la collecte de ses informations.

A noter : Les responsables de traitement doivent également respecter les règles strictes imposées en matière de profilage par le RGPD.

Sécuriser les données personnelles

Le responsable de traitement doit prendre les mesures nécessaires à la **sécurisation** des données personnelles afin de réduire les risques **de pertes de données** ou **de piratage** en respectant :

- Le principe de confidentialité : les données ne sont accessibles qu'aux personnes autorisées
- Le principe d'intégrité : les données ne doivent pas être altérées ou modifiées
- Le principe de disponibilité : les données doivent être en permanence accessibles aux personnes autorisées

Attention : Si l'association subit une **violation de données**, il faut procéder à un signalement à la CNIL dans les 72 heures suivant cette dernière si elle est susceptible de représenter un risque pour les droits et libertés des personnes concernées. Cette notification s'effectue en ligne sur le site internet de la CNIL.

Plusieurs mesures de sécurité peuvent être mises en place pour assurer la sécurisation des données : **le chiffrement** des données, **la pseudonymisation** des données.

A noter : Outre les étapes mentionnées, les associations peuvent également avoir recours à une formation RGPD. Celle-ci permet alors de mettre en place des mesures assurant la **mise en conformité** au RGPD de l'association.

Quelles sont les sanctions encourues en cas de non-conformité d'une association au RGPD ?

Si une association est dans une situation de **non-conformité** au RGPD, elle peut subir des sanctions prononcées par la CNIL. Elle risque notamment une sanction pécuniaire allant **jusqu'à 20 millions d'euros** ou **4% du chiffre d'affaires** annuel mondial.

Les autorités de contrôle peuvent également appliquer des **sanctions administratives** conséquentes et dissuasives, notamment :

- Imposer une obligation de conformité
- Réaliser un rappel à l'ordre
- Limiter définitivement ou temporairement le traitement des données personnelles

A noter : Ces mesures répressives peuvent également faire l'objet **d'une publication** , entraînant de graves conséquences sur l'image de l'association.

FAQ

Pourquoi une association est-elle soumise au RGPD ?

Une association est soumise au RGPD lorsqu'elle traite des données à caractère personnel. Ainsi, si une association procède à la collecte, la conservation ou l'utilisation de données, elle est concernée par le RGPD. Elle doit alors respecter les règles instaurées par le RGPD.

Quel type d'association est concerné par le RGPD ?

Le type d'association n'a aucun impact sur le respect du RGPD. En effet, le critère déterminant pour le respect du RGPD est le traitement de données personnelles. Ainsi, si une association traite des données, elle sera soumise au RGPD. Il importe peu que ce soit une association de loi 1901 ou une association reconnue d'utilité publique.

Comment mettre son association en conformité avec le RGPD ?

Les associations sont dans l’obligation de se conformer aux dispositions du RGPD. Pour cela, il est recommandé aux associations de tenir un registre de traitement des données. Elles doivent également veiller à respecter les droits des personnes tels que le droit d’opposition ou le droit à l’effacement.