joinly

Le guide du RGPD en milieu associatif

Avec le parrainage du

MINISTÈRE CHARGÉ DES SPORTS

Liberté
Égalité
Fraternité

Sommaire

Introduction

Le Règlement Général sur la Protection des données (RGPD) est en vigueur depuis le 25 mai 2018. Applicable dans toute l'Union européenne, il instaure un ensemble de règles dont l'objectif est de protéger les personnes physiques en ce qui concerne le traitement et l'exploitation de leurs données à caractère personnel.

Depuis 2018, les personnes morales, c'est-à-dire les entreprises, mais également tous les organismes qui recueillent régulièrement des données, ont dû mettre en place de nouvelles pratiques pour se conformer à ces obligations et éviter des sanctions administratives. **Les associations ne sont pas exclues de la législation autour du RGPD.** Si certaines se tiennent à l'écart parce qu'elles n'ont pas ou peu de données à traiter, d'autres ont encore du mal à percevoir les limites réglementaires du traitement des données de leurs membres. Ces interrogations sont légitimes puisque les textes de loi ne donnent pas précisément de clés ou de bonnes pratiques à mettre en place pour devenir une association « RGPD friendly ».
En fait, le RGPD est vu par beaucoup d'entreprises comme une réglementation commerciale, à tort. Le milieu de l'entreprise transmet cette croyance aux associations qui, elles, sont peu nombreuses à utiliser les données clients dans un but marketing et ne sont pas en quête de bénéfices.

Cependant, **le RGPD concerne seulement et uniquement les données dites à caractère personnel**, qu'elles soient à vocation commerciale ou simplement informative. Les associations sont donc directement concernées.

D'un autre côté, les associations comme les petites entreprises perçoivent le RGPD comme un ensemble de textes de loi complexes. Plus particulièrement, l'obligation de recueillir le consentement des personnes n'est pas toujours bien comprise. Dans ce livre blanc, nous aborderons en détail les contours de l'application du RGPD : Quelles sont ses obligations ? Qui est concerné ? Dans quelles situations le RGPD est-il la norme ?

Puis, nous nous focaliserons sur les obligations du RGPD en milieu associatif. Parce que nous connaissons bien votre quotidien, nous verrons quelles obligations du RGPD vous concernent particulièrement, en laissant de côté celles qui sont plutôt relatives aux activités commerciales.

Pour répondre à ces obligations, Joinly vous propose de suivre un ensemble de bonnes pratiques RGPD, à mettre en place sans plus attendre pour améliorer la façon dont vous traitez les données de vos membres. Enfin, parce qu'il nous faut bien vous prévenir, nous vous avons prévu un zoom sur les sanctions en cas de non-conformité à la RGPD. Mais promis, vous devriez pouvoir éviter cela facilement en suivant le guide !

‘ Le RGPD instaure un ensemble de règles afin de protéger les personnes physiques et leurs données à caractère personnel ‘

CHAPITRE 1

Le RGPD en détail

Près de trois ans après l'instauration du RGPD, celui-ci fait toujours autant parler de lui. Pourtant, lorsqu'il s'agit de donner une définition, les choses se compliquent. Le RGPD souffre d'une image de texte complexe. Alors, concrètement, le RGPD, c'est quoi ?

RGPD : une législation européenne plus simple qu'il n'y paraît

Le Règlement Général sur la Protection des données est le texte de référence européen en matière de traitement des données pour tous les résidents de l'Union européenne. Et c'est tout ? Oui, enfin en ce qui concerne le texte de loi. Car **celui-ci a amené avec lui un ensemble d'obligations qui forme ce que l'on appelle parfois la « norme RGPD ».**

Dans un premier temps, la définition du terme RGPD a peu de sens si l'on n'a pas connaissance du terme de « données à caractère personnel ». En effet, cette notion est centrale dans le RGPD. Alors, une donnée à caractère personnel, qu'est-ce que c'est ?

Selon la CNIL, une donnée personnelle se définit comme « toute information se rapportant à une personne physique identifiée ou identifiable ». Dans le quotidien des organisations qui récoltent des données, il peut s'agir d'éléments comme :

- le nom et/ou le prénom ;
- un numéro d'identification : numéro de pièce d'identité, de sécurité sociale, de dossier, identifiant en ligne, etc. ;
- une donnée de localisation : adresse de résidence ou géolocalisation, par exemple.

Parmi les données à caractère personnel, certaines sont reconnues par le RGPD comme des **données sensibles**. Selon la législation, elles doivent faire l'objet d'une sécurisation plus importante. Il s'agit des catégories de données qui révèlent :

- l'origine prétendument raciale ou ethnique de la personne ;
- ses opinions politiques, philosophiques ou religieuses ainsi que l'appartenance syndicale ;
- a santé ou son orientation sexuelle ;
- des données génétiques ou biométriques ;
- des données sur les éventuelles infractions ou condamnations pénales de la personne.

En soi, le RGPD est une réglementation relativement simple, qui porte sur l'usage des données personnelles par les organisations de toute sorte. Son but principal est de **protéger la liberté fondamentale de chaque individu à disposer des données qui le concernent**.

En réalité, ce qui rend le RGPD complexe, ce sont les différents contextes au sein desquels il se développe. Comme tout cadre législatif, il détermine un certain nombre d'obligations communes à des structures très différentes. Mais sur le terrain, les enjeux liés à la protection des données sont très nombreux. C'est ce qui explique, notamment, que les organisations associatives se sentent encore à l'écart des informations qui circulent sur la mise en pratique du RGPD.

Zoom sur les obligations du RGPD

Cette partie a vocation à présenter **le cadre législatif strict du RGPD**. C'est-à-dire les obligations qui composent la réglementation, et qui concernent tous les types de structures professionnelles.

Tout d'abord, la norme RGPD détaille plusieurs types d'obligations :

- une obligation générale de sécurité et de confidentialité ;
- une obligation d'information ;
- une obligation de mener une analyse d'impact sur la vie privée (PIA) en cas de collecte de données reconnues comme sensibles ;
- une obligation de désigner un délégué à la protection des données (DPO) ;
- une obligation de tenir un registre des traitements de données.

Globalement, ces obligations imposent aux organismes de mettre en œuvre des mesures de sécurité à la fois dans leurs locaux et dans leurs systèmes d'information pour protéger les fichiers contenant des données sur des tiers, c'est-à-dire sur des personnes physiques ayant été en interaction avec la personne morale en question.

Le RGPD ne prend pas du tout en considération la dimension commerciale. On ne parle donc pas de recueillir le consentement des clients, même si pour les entreprises, c'est évidemment l'enjeu dont il est question.

Au sein de l'organisme soumis au RGPD, le délégué à la protection des données (désigné en interne au préalable) a pour rôle de concevoir ces mesures et de les faire appliquer à tous les niveaux de l'organisation. Il est tenu, entre autres, à un principe de minimisation qui indique que l'organisme doit s'efforcer de limiter le nombre de données collectées. Parmi les autres points importants du RGPD, le DPO doit également pouvoir, à tout moment, faire preuve de sa conformité avec la législation et renseigner les administrations sur la finalité et le contexte des actions de récolte de données.

Quelles sont les structures concernées ?

Le RGPD s'applique très largement et sans exception dès lors que :

- une organisation traite des données personnelles ;
- un résident de l'UE est concerné par un traitement de données à caractère personnel.

En somme, la réglementation s'applique de la même manière à tous les organismes quels que soient leur taille, leur secteur ou leur caractère public ou privé, c'est-à-dire :

- les entreprises ;
- les organismes publics ;
- les associations ;
- une obligation de désigner un délégué à la protection des données (DPO) ;

L'intégration des sous-traitants dans la législation et le contrôle de la manière dont ces organismes recueillent et exploitent les données a représenté l'un des changements majeurs à l'arrivée du RGPD. Désormais, les sous-traitants des entreprises publiques et privées, mais également des associations sont dans l'obligation de se soumettre au RGPD, même s'ils exercent en dehors de l'Union européenne.

Les sous-traitants ont également une obligation de conseil et d'aide au respect du RGPD auprès de leurs entreprises clientes. Une entreprise sous-traitante qui transmet des données confidentielles à son entreprise cliente doit donc mettre en œuvre tous les moyens à sa disposition pour sécuriser ces dernières. Si des manquements sont constatés, le responsable du traitement de l'entreprise cliente et le sous-traitant peuvent tous deux être sanctionnés.

Dans les faits, l'ampleur du travail de sécurisation des données pour une organisation ne dépend pas directement du volume de données traitées, mais surtout du caractère sensible des données qu'elle exploite. Ainsi, une entreprise qui opère dans le domaine de la santé, et possède donc des bases de données patients contenant des informations très confidentielles, pourrait faire face à un processus de mise en conformité avec le RGPD bien plus conséquent qu'un grand magasin, qui possède certes beaucoup de clients mais qui recueille des données plus générales, dont le niveau de sensibilité est moindre.

'La réglementation s'applique de la même manière à tous les organismes quels que soient leur taille, leur secteur ou leur caractère public ou privé'

Dans quel contexte une association peut-elle être soumise aux normes RGPD ?

Comme présenté ci-dessus, les associations sont directement concernées par le RGPD. Bien entendu, tous les aspects de la réglementation ne s'appliquent pas forcément à leur activité. Une association ne ressemblant pas à une autre, il est donc normal de constater des différences d'enjeux de sécurisation des données. Mais là encore, il peut y avoir des pièges. Si, en tant que président(e) d'association, vous pensez que le RGPD ne s'applique pas à votre structure, il y a peut-être des aspects de la réglementation que vous n'avez pas envisagés. Pas de panique, nous allons remédier à cela. Il y a en réalité plusieurs contextes-types dans lesquels une structure associative est très directement soumise au RGPD sans forcément en avoir conscience.

Par exemple, une petite association qui a pour projet de refaire son site internet se rend compte qu'elle doit exploiter des données pour présenter la vie associative, ses actions sur le terrain, etc. Bref, communiquer ! Pour prouver qu'elle est dans la légalité vis-à-vis du RGPD, son site web devra intégrer des mentions d'informations, également appelées « mentions légales ». Celles-ci doivent absolument mentionner les éléments suivants :

- l'auteur de la collecte de données ;
- la durée de conservation des données ;
- la finalité des données collectées : « à quoi vont-elles servir ? » ;
- les informations relatives aux droits des personnes dont les données ont été utilisées.

Il ne s'agit là que d'un exemple, et la création d'un site internet n'est pas le seul contexte dans lequel une association doit montrer qu'elle se soumet aux obligations du RGPD. Par ailleurs, les obligations du RGPD qui concernent directement le milieu associatif peuvent être regroupées en 5 catégories, que nous allons développer dans la partie suivante. **Pour connaître vos obligations au regard de la RGPD en tant que responsable d'association, rendez-vous à la partie suivante !**

CHAPITRE 2

Les obligations RGPD du milieu associatif

Nous l'avons vu, les associations ne sont pas oubliées par le RGPD. Celui-ci s'applique dans le cadre professionnel au sens large. Pour exercer, une association a dû dans un premier temps déposer des statuts, qui concrétisent son action sur le terrain. La plupart des structures associatives sont aujourd'hui couvertes par la loi 1901. Elles sont reconnues comme des organisations professionnelles à part entière. Assez logique, lorsque l'on sait que les associations peuvent employer des salariés. La grande majorité des obligations RGPD formulées par la CNIL en 2018 s'appliquent donc au milieu associatif. Les voici mises en contexte afin de vous aider à évaluer votre conformité au RGPD.

Trier régulièrement les données

Le RGPD impose un tri régulier des données, qui va de pair avec la constitution d'un registre de traitement des données sur laquelle nous reviendrons par la suite, au moment de vous délivrer les bonnes pratiques d'une association en phase avec le RGPD.

Trier ses données, en quoi cela consiste ? C'est simple : il s'agit de faire un grand ménage pour répondre à l'obligation, évoquée précédemment, de ne **récolter que des données utiles et pertinentes vis-à-vis des objectifs de l'association**. Cela revient à se débarrasser de toutes ces choses que l'on entasse au grenier et dont on ne se sert finalement jamais. Dans ce genre de processus, pas question de se mentir, ou bien les vieux bibelots pourraient rester à leur place pendant encore quelques années. Au moment de trier les données dans votre association, demandez-vous quel intérêt elles ont pour vos objectifs de développement actuels. Cela vaut aussi bien pour des données numériques ou des documents papiers, même si dans le premier cas, on a plus tendance à repousser l'épreuve du tri à plus tard.

Petit à petit, en mettant en pratique les obligations édictées par le RGPD, vous entrerez dans une logique d'économie. En effet, moins de données collectées correspond à moins de risques d'erreurs. Plus généralement, gardez à l'esprit que ce qui compte le plus en RGPD est de **montrer que vous ne collectez pas de données avec de mauvaises intentions, et que vous êtes dans une démarche d'amélioration constante**.

Détenir un registre de traitement des données

Qui dit trier ses données, dit aussi les conserver ! Et n'est-il pas plus facile de ranger une fois débarrassé de quelques objets encombrants ? Le registre de traitement des données, c'est un peu ce placard bien rangé qui vient de subir un grand ménage de printemps. Plus sérieusement, il s'agit d'un document qui a peu à peu pris une valeur officielle à mesure que le RGPD a fait sa place dans le traitement des données. Pour les associations, c'est un outil précieux qui permet d'organiser le tri et la mise à jour des données et de prouver leur conformité en cas de contrôle par les autorités.

Le registre de traitement des données se présente généralement sous la forme d'un tableau. Si votre association a investi dans un CRM pour piloter son activité, ce registre peut être mis en place dans l'outil. Il sera alors directement lié aux bases de données de l'association, auxquelles, rappelons-le, celle-ci doit pouvoir accéder si une personne lui demande de supprimer des données personnelles la concernant, comme le mentionne le RGPD.

Organiser la collecte du consentement

L'une des formalités essentielles du RGPD est la collecte du consentement des personnes. C'est ce qui fait que depuis 2018, des bandeaux ou pop-up nous demandent, sur chaque site internet visité, si nous acceptons les cookies. Mais Internet n'est pas le seul espace dans lequel la collecte du consentement est devenue une obligation.

Quelle que soit sa forme, **le consentement doit être clair** afin de démontrer en toute transparence que la personne a accepté de partager ses données personnelles avec vous en ayant, en retour, connaissance des modalités d'exploitation de ces mêmes données. Pour plus de précision, vous pouvez faire mention du canal ou de l'outil pour lequel les données seront utiles. Par exemple, lors de l'inscription d'un utilisateur à votre newsletter, demandez-lui simplement s'il accepte que son adresse e-mail soit utilisée pour lui envoyer d'autres contenus. **Restez transparent et n'hésitez pas à répondre de manière détaillée** à quelqu'un qui souhaiterait obtenir plus d'informations sur la finalité de la récolte de données.

Protéger les données collectées

En matière de RGPD, **une association est considérée de la même façon que tous les autres détenteurs de données personnelles**. Via un DPO désigné en interne si cela est nécessaire (ce point sera évoqué au moment d'aborder les bonnes pratiques RGPD pour une association) ou par le ou la président(e) d'association, le rôle de l'association est de protéger et de sécuriser ces données.

Aujourd'hui, la majorité des données personnelles sont stockées sur des bases de données, elles-mêmes hébergées sur des serveurs. En tant que responsable de la sécurisation, **l'association doit donc prendre le temps de bien choisir son hébergeur** afin de limiter les éventuelles failles de sécurité, qui viendraient mettre en péril les données plus ou moins sensibles de ses membres. Pour cela, quelques bonnes pratiques doivent devenir des habitudes. Chiffrage de données, installation d'un antivirus adapté au nombre de données traitées, mise en place de mots de passe robustes etc. Là encore, on vous en dit plus dans la partie suivante. Des procédures peuvent vous permettre de mettre les données de vos membres à l'abri facilement et ainsi maintenir une relation de confiance essentielle avec eux.

CHAPITRE 3

Association : les bonnes pratiques pour devenir « RGPD friendly »

Vous avez pris connaissance de vos obligations en tant qu'association et vous souhaitez mettre en place de nouvelles pratiques pour mieux respecter le RGPD ? Voici quelques outils qui devraient vous y aider.

Désigner un DPO (Data Protection Officer)

Le terme DPO - pour l'anglais « Data Protection Officer » - désigne **la personne choisie dans l'association pour prendre en charge toute la dimension RGPD**. Bien qu'elle ne soit pas obligatoire pour une association, la désignation d'un responsable du traitement des données n'est pas une tâche à prendre à la légère. Dans le respect de la réglementation RGPD, elle a une valeur juridique et administrative. En cas de contrôle, c'est cette personne qui devra répondre aux sollicitations. Elle doit donc bien connaître les process de l'association en ce qui concerne l'application du RGPD et si cette dernière n'en dispose pas encore, les mettre en place.

Si vous êtes président(e) d'association, vous n'êtes bien sûr pas dans l'obligation de prendre en charge ce rôle. D'ailleurs, il est plutôt conseillé de désigner un DPO parmi les membres actifs qui ont un bon niveau de familiarité avec les outils numériques. Bien que le RGPD s'applique également aux documents papiers, la personne responsable du traitement des données ne doit pas avoir peur de manipuler des bases de données, ou encore d'installer des logiciels anti-virus sur le site web de l'association.

Au-delà de ces compétences techniques, le futur responsable du traitement des données doit s'intéresser au RGPD, être ouvert à l'apprentissage de nouvelles réglementations, et faire preuve de rigueur et d'organisation. Comme dans tous les processus de mise en conformité, le plus important est de piloter les actions de manière minutieuse afin de limiter la marge d'erreur.
On vous l'accorde, la gestion du RGPD ne fait pas rêver tous les bénévoles d'association. Cela devrait permettre de faire le tri au sein de vos membres les plus actifs. Quel que soit votre choix, assurez-vous que la personne désignée présente un vrai attrait pour la question de la protection des données personnelles. Elle pourra alors vous mettre au courant des évolutions à ce sujet, et vous gagnerez en sérénité.

Au quotidien, le DPO se fait le chef d'orchestre de la conformité de l'association au RGPD. Il est en charge :

- d'informer et de conseiller les équipes et le responsable d'association sur la réglementation.
- de s'assurer que le RGPD et plus globalement, le droit national sont respectés dans les actions courantes de l'association.
- de conseiller le/la président(e) d'association sur la conduite d'une analyse d'impact relative à la protection des données (PIA) si cela est nécessaire, et de vérifier que celle-ci est bien menée.
- de coopérer avec les autorités et les organismes de contrôle et d'être le point de contact en ce qui concerne l'application du RGPD.

Une fois que vous avez trouvé la perle rare et désigné votre DPO, vous allez pouvoir, main dans la main, passer en revue l'ensemble des pratiques de votre association en ce qui concerne le traitement des données personnelles. Alors, prêts ?

Cartographier les données et leurs ressources

À son arrivée en poste, **le DPO a pour mission d'analyser et de répertorier les données que votre association utilise ou conserve**. La cartographie des données consiste à mener une enquête en interne. Elle peut nécessiter de demander à d'autres membres actifs de l'association de coopérer. L'objectif est de vous demander : « Quelles autres personnes ont accès à ces données ? » et « Est-ce que ces personnes sont autorisées à disposer de ces données ? »

La cartographie des données va de pair avec le registre des traitements évoqué dans la partie précédente. Ce document permet de **sourcer les données dont dispose votre association et de préciser la manière dont elles sont utilisées**. Si vous n'avez pas tenu de registre de traitement des données jusqu'à présent, pas de panique. Il n'est jamais trop tard pour bien faire ! Pour commencer à cartographier vos données, posez-vous les questions suivantes :

Quelles sont les données personnelles dont l'association dispose ? Nom ? Prénom ? Adresse email ? Adresse postale ? Informations personnelles sur l'âge, l'activité professionnelle, la situation familiale etc. ?

Comment ces données ont-elles été acquises ? Via une inscription en ligne, via des cartes de visite ou des flyers distribués dans la rue ? Ou bien par téléphone ?

Où les données sont-elles hébergées ou archivées ? Sur un ordinateur ? Sur un logiciel en ligne de type CRM ? Sur un téléphone appartenant à l'association ?

Quelle utilisation faites-vous de ces données ? Les utilisez-vous pour formuler des appels au don ? Pour inviter vos membres à des événements ? Pour faire appel à des bénévoles pour vos prochaines actions ?

Qui peut accéder à ces données personnelles ? Tout le monde ? Seulement l'administration de l'association ? Y a-t-il des codes d'accès pour y accéder ?

Combien de temps les données personnelles sont-elles conservées ? Depuis le moment où vous avez recueilli chacune d'entre elles, ou bien depuis l'année dernière ?

On vous l'avait dit : c'est une véritable enquête que doit mener le DPO en fonction des réponses à toutes ces questions, et à d'autres en fonction des besoins de votre association. Le DPO va mettre en place des processus adaptés à la vie quotidienne de votre association, mais aussi à la manière dont vous traitiez les données jusqu'alors.

En tant que responsable de la mise en place d'une vraie politique RGPD dans l'association, le DPO instaure des processus spécifiques pour chaque type de traitement de données. Ainsi, les données issues de la prospection téléphonique n'auront pas le même traitement que les informations fournies à l'association lors d'une inscription à sa newsletter, par exemple.

Ce qui fait la différence de traitement entre ces types de données, c'est la manière dont a été recueilli le consentement de la personne.

Prenons un exemple concret : un club de football désire lancer une campagne de communication autour de ses activités pour agrandir son nombre de membres et ainsi se développer. Pour cela, il met en place un système de parrainage. Celui-ci consiste, pour les membres actuels de l'association, à inviter des amis à s'inscrire à la newsletter du club afin de recevoir en échange une réduction sur le montant de leur cotisation annuelle. Lorsqu'un nouvel abonné s'inscrit, il renseigne quelques informations sur son profil.

Dans le cadre de cette campagne, le club a précisé que les données seraient utilisées dans le but de mettre en place des cours d'essai par niveau sportif. À l'issue de ces différents cours d'essai, les abonnés à la newsletter peuvent choisir de souscrire à une adhésion annuelle dans le club de football. Dans ce cas précis, la mise en place d'un formulaire numérique a permis au club de football de recueillir un consentement clair et transparent en ligne. Si l'administration du club avait téléphoné à des listes de contacts pour leur proposer de s'inscrire à un cours d'essai de football, elle n'aurait non seulement pas obtenu les mêmes résultats, mais elle n'aurait pas eu à mettre en place la même cartographie de données. L'objectif ? Assurer une traçabilité de chaque donnée.

Bien entendu, le DPO n'est pas présent dans toutes les missions de l'association qui nécessite d'appliquer le RGPD. En réalité, le RGPD est présent partout. Pour s'assurer qu'il soit bien mis en place, le DPO doit faire en sorte de **mener des actions de sensibilisation auprès de l'ensemble des membres de l'association**, et en particulier des membres administratifs. Le but ultime ? Que chacun connaisse le champ d'application du RGPD correspondant à ses missions.

Prêter une attention particulière aux données sensibles

Comme nous l'avons vu auparavant, les données sensibles sont une catégorie de données personnelles qui nécessitent une plus grande vigilance. Les associations ne sont pas exclues de la réglementation spécifique concernant les données sensibles.

Une donnée sensible est une information apportant des indications sur l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou encore l'appartenance syndicale d'une personne. Une donnée sensible peut être une donnée génétique ou biométrique, permettant de distinguer une personne physique parmi d'autres.

Les données relatives à la santé sont les données sensibles les plus courantes. Elles peuvent concerner directement le monde associatif. Par exemple, notre club de football peut avoir en sa possession des données sensibles sur l'état de santé de ses joueurs. Si une blessure a lieu sur les terrains du club, par exemple, il se peut que l'administration possède des données relatives aux circonstances de l'accident. Elle devra donc redoubler de vigilance pour sécuriser l'accès à ce type de données, qui peuvent révéler des informations sensibles sur un membre.

Le RGPD interdit globalement de recueillir ce type de données. C'est la raison pour laquelle si un joueur est suspendu de jeu dans ce même club de football, il n'a pas à donner de justification médicale précise. Dans ce cas, le RGPD complète l'obligation au secret médical.

Le RGPD interdit également d'utiliser des données sensibles quelles qu'en soient les fins. Elle prévoit certaines exceptions si :

- La personne a donné son consentement au cours d'une démarche explicite, de préférence sur un support écrit, et de son plein gré.
- La personne concernée à elle-même rendu ses informations publiques.
- L'utilisation de ces données sensibles est justifiée par un intérêt public.
- Les données concernent les membres ou adhérents d'une association ou d'une organisation politique, religieuse, philosophique, politique ou syndicale.

Vous l'aurez compris, les associations sont directement concernées par les clauses spécifiques du RGPD sur les données sensibles. En effet, les données sensibles qui concernent directement l'action de l'association bénéficient d'un traitement différent. Dans ce cas de figure, c'est le bon sens qui prédomine pour appliquer correctement le RGPD. Si nous parlons d'une association politique, il est relativement logique que le ou la président(e) de l'association dispose d'informations sur l'orientation politique de ses militants. En revanche, chaque personne conserve le droit à la modification ou à la suppression de ses données personnelles. **Un membre qui quitte une association peut demander à ce que les données qui le concernent soient effacées**.

'Les associations sont directement concernées par les clauses spécifiques du RGPD sur les données sensibles'

Conformer les documents de l'association au RGPD

Contrairement à ce que l'on peut être tenté de penser, **le RGPD s'applique à toutes les données collectées quel que soit le suppor**t. Ainsi, les fichiers papiers sont concernés. Si votre association a quelques années d'activité derrière elle et que vous avez conservé des dossiers par ordre alphabétique dans de gros classeurs, vous savez ce qu'il vous reste à faire ! Cependant, même s'il n'y a pas de règles précises sur la durée de conservation des données, il est plutôt conseillé de vous débarrasser des fiches des membres qui œuvraient dans votre association il y a une vingtaine d'années.

- Imaginons que notre club de football soit intraitable sur les questions de RGPD. Chaque année, le club accueille de nouveaux membres. Il fait remplir une fiche d'informations à chaque nouvel inscrit. A chaque rentrée, il a pris l'habitude de détruire les fichiers papier correspondant aux fiches de ses anciens joueurs de football. En ce qui concerne les registres informatiques, son CRM gère tout. En début d'année, les responsables de l'administration de l'association ont simplement à indiquer quels membres restent adhérents, afin que leurs informations soient conservées. Les autres sont supprimées automatiquement.

La mise en conformité des documents de l'association vis-à-vis du RGPD fait partie des bonnes pratiques à mettre en place. Celles-ci demandent, certes, d'automatiser les processus et il est normal d'avoir des difficultés à le faire rigoureusement dans les premiers temps.

Pour prendre le pli, n'hésitez pas à vous appuyer sur des outils pensés pour le monde associatif. Aussi, dans toutes vos actions de collecte de données, **assurez-vous de respecter le principe de minimisation des données**. Quand vous produisez un document tel qu'un bulletin de don par exemple, demandez-vous s'il est bien nécessaire de recueillir la date de naissance de la personne. On vous l'assure, au bout de quelques mois, ces questionnements vous viendront naturellement.
dans une démarche d'amélioration constante.

Structurer la gestion des données par des procédures internes

La gestion des données est une activité chronophage qui nécessite de mettre en place des processus structurés. Le RGPD fait mention de l'importance de sécuriser les données personnelles et plus concrètement, de limiter les risques en matière de cybersécurité. En effet, **c'est sur internet que la sécurisation des données présente l'enjeu le plus important**.

Les risques sur Internet sont nombreux : espionnage, usurpation d'identité, fraude, attaque informatique via les mails où le site web, virus ou hameçonnage.

Pour faire face à ces menaces de plus en plus ciblées et spécifiques, il vous faut mettre en place des actions de sécurisation structurelles. C'est-à-dire des règles qui vous sont propres, sur la gestion des accès aux fichiers protégés, avec une hiérarchisation des personnes qui sont autorisées à y accéder, la mise en place de mots de passe robustes en fonction du niveau de sensibilité des documents, ainsi qu'une sécurisation générale des réseaux (dont s'occupe généralement le prestataire auquel vous avez souscrit à un contrat d'hébergement).

En tant que président(e) d'association, vous êtes également tenu de **notifier toute faille de sécurité à la CNIL**. Là encore, ce type d'incident doit faire l'objet d'un processus entendu par toutes les parties prenantes de l'association sur les questions de traitement des données.

- Par exemple, le processus peut être le suivant : le DPO se charge lui-même de sécuriser le site internet du club de football dès lors qu'il constate que celui-ci a subi une menace. Rapidement, il doit aussi en informer le/la président(e) de l'association. Si cette règle a été approuvée par tous en interne au préalable, il n'y a pas de raison que la protection des données ne soit pas bien appliquée en cas de menace.

Si vous travaillez avec des fournisseurs, prenez le temps d'inclure les normes RGPD dans le contrat que vous passez avec eux. Si les données que vous partagez avec votre fournisseur sont relativement sensibles, optez pour une clause contractuelle sur les types de protection. Si le prestataire en question exerce en dehors de l'UE, redoublez d'autant plus de vigilance.

CHAPITRE 4

Les sanctions en cas de non-conformité de l'association au RGPD

Tout d'abord, rassurez-vous. Si vous n'êtes pas encore tout à fait en règle avec le RGPD, vous ne risquez pas de voir votre association fermée dans les prochains jours. Les associations ne représentent pas la cible principale de la réglementation générale sur la protection des données. Celle-ci vise avant tout les entreprises commerciales, même si elle n'exclut pas les structures associatives. Le RGPD est lié à des règles de bon sens : les données collectées à des fins publicitaires sont considérées comme prioritaires, et donc observées avec plus de sévérité de la part des autorités.

Ce qui compte, c'est de démontrer en cas de contrôle que vous avez mis en place une démarche pour respecter la réglementation en vigueur. Car oui, la CNIL est en droit de contrôler votre conformité avec le RGPD de différentes manières. Il peut s'agir d'une visite dans les locaux de l'association, d'un contact par téléphone, d'un contrôle sur votre site internet ou encore d'une convocation à une audition.

Attention, il n'est pas question de mettre de la poudre aux yeux aux autorités. Lors de la mise en place du RGPD en 2018, précisément un mois après son entrée en vigueur, l'ADEF (Association Départementale d'Études et de Formation) a été sanctionnée à la suite d'une faille de sécurité qui concernait son site web. Elle a reçu une amende d'un montant de 75 000 euros. Cette mesure a permis au monde associatif de prendre connaissance de ses obligations et des risques qu'il encourt en cas de non-conformité avérée. Dans les faits, les sanctions restent de l'ordre de l'administratif si aucune plainte n'a été enregistrée de la part de personnes concernées par une collecte de données de votre part.

Les sanctions administratives

La CNIL est en mesure de prononcer diverses sanctions administratives qui correspondent à différents niveaux de gravité du manquement aux obligations du RGPD. Ces sanctions sont applicables en plusieurs étapes. C'est la raison pour laquelle nous vous avons précisé que, si vous êtes dans une démarche d'amélioration de votre politique RGPD et que vous prouvez que vous avez mis en œuvre des actions pour soigner le traitement de vos données, vous ne devriez pas être inquiété. Ces étapes sont les suivantes :

1. Un avertissement ou une mise en demeure de l'association et un rappel à l'ordre, qui peut prendre la forme d'un courrier, d'un mail ou d'un appel téléphonique ;

2. Une injonction à cesser le traitement des données si la manquement le manquement persiste ;

3. Une limitation ou une suspension des flux de données par la CNIL ;

4. Une demande à effacer les données qui ont été recueillies de façon illicite ;

5. Un ordre de respecter les droits des personnes, c'est-à-dire rappel à la loi sur les libertés fondamentales et individuelles de disposer de ses propres données à caractère personnel ;

6. Et en dernier lieu le paiement d'amendes administratives qui peuvent aller jusqu'à une dizaine de millions d'euros en fonction de la gravité de la non-conformité au norme RGPD et de l'ignorance, par l'association, des étapes précédentes.

Plus spécifiquement, **les sanctions administratives s'appliquent à des groupes d'infractions** :

- Le non-respect des obligations du responsable du traitement, c'est-à-dire soit le DPO, soit le gestionnaire de l'association si aucun responsable du traitement des données n'a été désigné ;
- Le non-respect des obligations RGPD d'un sous-traitant.

Ces deux types d'infractions sont sanctionnées par une amende de l'ordre de 10 millions d'euros, ou de 2 % du chiffre d'affaires global de l'association.

D'autres types d'infractions font appel à des sanctions administratives :

- Le non-respect de l'obligation de recueillir le consentement des personnes ;
- Le non-respect des droits fondamentaux des personnes concernées par la collecte de données ;
- Le non-respect de la mise en place de certaines mesures relatives au RGPD après que celle-ci ait été demandée via un ordre prononcé par la CNIL.

Pour ces trois infractions, l'amende est de 20 millions d'euros ou de 4 % du chiffre d'affaires mondial de l'association. Par ces critères de sanction, la CNIL veut démontrer que les petites associations, bien qu'elles traitent un nombre plus faible de données, ne sont pas exemptes de mettre en place des démarches pour améliorer le traitement de leurs données.

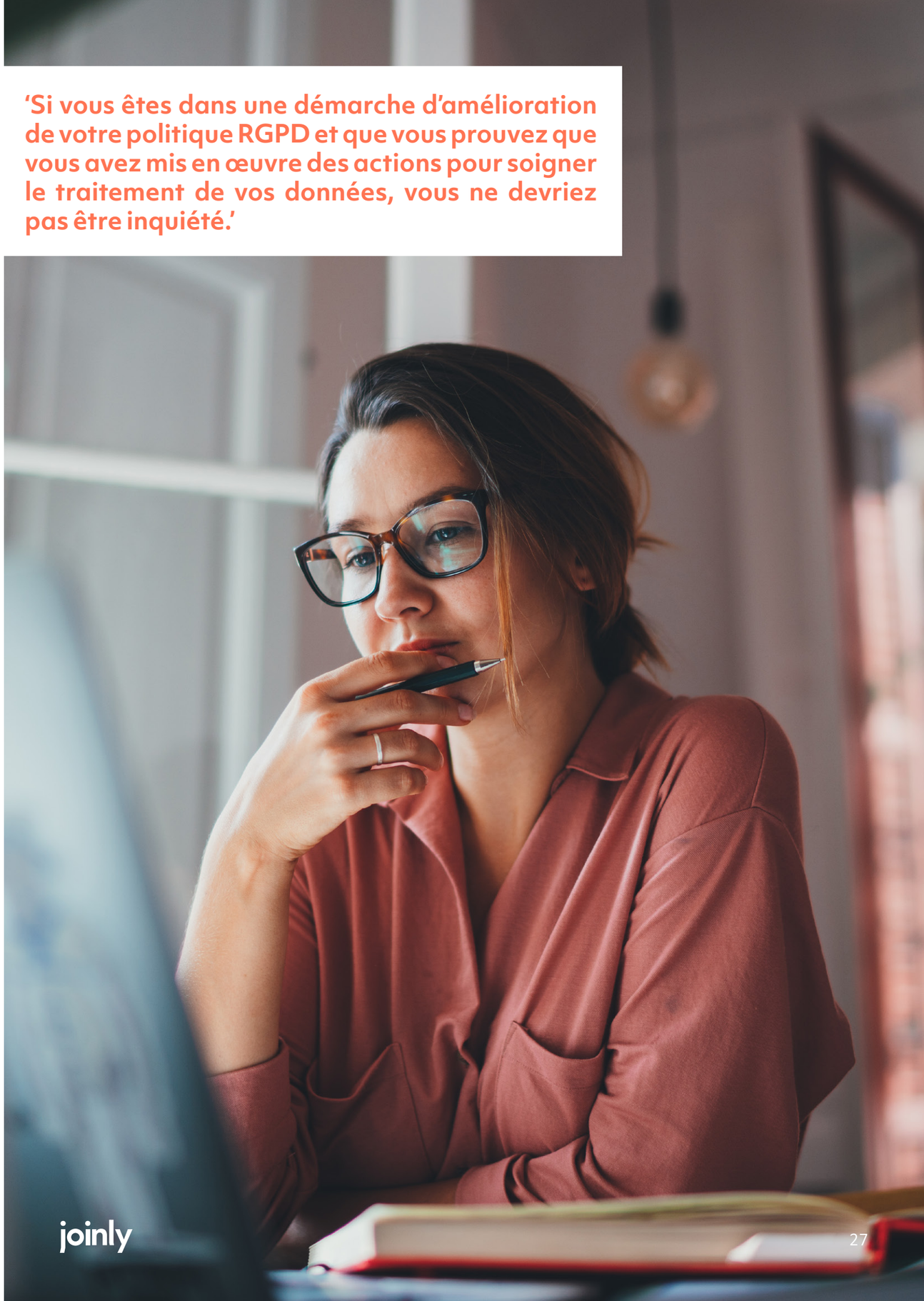
Les sanctions pénales

En droit, les sanctions pénales sont la conséquence d'un recours en justice. En ce qui concerne le RGPD, une association sanctionnée par une amende administrative, quel que soit son montant, peut aussi faire l'objet d'une poursuite judiciaire, à la suite de sanctions pénales si des victimes ont porté des manquements jusqu'à la justice.

Dans ce type de cas particulier, **le RGPD agit en tant que norme, sur laquelle les manquements sont constatés**. Le plaignant peut alors s'appuyer sur cette réglementation européenne pour justifier son accusation et démontrer que ses droits à disposer pleinement de ses données personnelles n'ont pas été respectés. Cependant, dès lors que la plainte est déposée en justice, c'est le droit français qui prend le relais. Le RGPD est un règlement européen parmi d'autres et ne se substitue pas à la loi du pays dans lequel l'infraction est relevée.

L'article 84 du RGPD mentionne : *« Les États membres déterminent le régime des autres sanctions applicables en cas de violation du présent règlement, en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 83, et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre. Ces sanctions sont effectives, proportionnées et dissuasives. »*

'Si vous êtes dans une démarche d'amélioration de votre politique RGPD et que vous prouvez que vous avez mis en œuvre des actions pour soigner le traitement de vos données, vous ne devriez pas être inquiété.'



Conclusion

Que retenir ?

Alors, RGPD et milieu associatif, inconciliables ? Depuis son instauration en 2018, le RGPD est toujours soumis à des questionnements de la part du monde associatif. Mais, si cela peut vous rassurer, les choses ne sont pas tellement plus claires du côté des entreprises...

Depuis trois ans, ces entreprises comme les associations ont dû mettre en place de nouvelles pratiques pour répondre à cette obligation de transparence et de respect vis-à-vis des personnes physiques sur le traitement de leurs données, considérées comme un droit inaliénable.

En tant qu'association, **la gestion de l'application du règlement général de la protection des données représente un temps conséquent**, à prendre en compte dans l'organisation quotidienne de la structure. Elle impacte non seulement le travail du ou de la président(e) d'association, mais aussi de tous les membres du bureau et du conseil d'administration.

Alors, comment faire en sorte que le RGPD ne représente pas une contrainte dans le fonctionnement courant de l'association ? Tout d'abord, comme nous vous l'avons présenté, **le rôle du DPO est essentiel.** Bien que celui-ci ne soit pas obligatoire pour les associations, le DPO a un rôle considérable dans l'orchestration de la mise en œuvre des pratiques autour du RGPD. Il est donc primordial de bien définir les rôles de chacun avant de se lancer dans une démarche de mise en conformité avec le RGPD.

Pour organiser la mise en œuvre d'une démarche RGPD sur le long terme, **l'association peut s'appuyer sur ses outils courants de gestion**, qu'il s'agisse de protéger des données récoltées lors d'événements ou bien sur Internet. La mise en conformité RGPD demande dans un premier temps de poser les bases d'une politique de traitement des données, afin de n'avoir plus qu'à suivre des processus établis, par la suite.
Dans un premier temps **l'association doit procéder à un tri de ses données**, qu'elle devra renouveler régulièrement, en fonction de son propre emploi du temps, c'est-à-dire des temps forts de son activité.

Dans un second temps, **il est fortement conseillé à l'association de tenir un registre de traitement des données**. Ce document permet de centraliser les sources des données collectées ainsi que la manière dont elles sont traitées. Il ne s'agit pas d'un document officiel à proprement parler, mais il facilite la justification des moyens employés par l'association pour traiter les données.

> L'exemple du club de football a démontré que, pour lui, la période de la rentrée scolaire est propice à des actions de tri afin de se débarrasser des informations concernant les membres qui ne font plus partie de l'association. Ce type de démarche peut, avec le temps, devenir un ensemble d'habitudes permettant d'appliquer le principe de minimisation édicté par la réglementation en vigueur. En somme, si cette opération peut sembler très contraignante au départ, elle le sera de moins en moins à force de régularité.

D'autre part, l'organisation de la collecte du consentement répond au principe le plus évident du RGPD, plus particulièrement **celui du consentement des personnes à délivrer des données personnelles à une organisation**, quelles qu'en soient les fins. Pour conserver toute sa pertinence, le consentement doit faire l'objet d'une déclaration claire et transparente, de préférence à l'écrit. Pour être dans la loi, vous devrez également tenir chaque personne au courant des modalités d'exploitation de ses données personnelles.

Enfin, le dernier aspect porte sur les efforts déployés par une association pour **protéger les données collectées**. Lorsque ces données sont conservées sur des bases elles-mêmes hébergées par des serveurs, les processus de sécurisation peuvent prendre une dimension très technique.

En somme, pour parvenir à vos objectifs RGPD et, non seulement être en conformité avec la loi, mais aussi ancrer l'association dans une relation de confiance avec ses membres, quelques bonnes pratiques peuvent être instaurées relativement facilement et rapidement.
Tout d'abord, désignez une personne chargée de la protection des données. Il peut s'agir de ce que l'on appelle un DPO, ou bien d'une personne qui présente un intérêt pour les questions de protection des données, et dispose d'une bonne connaissance des actions de l'association.

Puis, attachez-vous à situer **une cartographie complète des données et de leurs ressources** à partir d'un simple registre de traitement des données, ou bien d'un outil interactif comme un CRM ou un ERP, permettant de construire des tableaux interactifs. Au-delà du fait de répondre à des obligations légales, vous comprendrez également mieux la manière dont la structure associative interprète et exploite les données qui sont mises à sa disposition. Si vous disposez d'un trop grand nombre de données, vous devriez ainsi vite vous en rendre compte.

Dans ce processus d'inventaire des données, portez une attention particulière aux données sensibles. Les données sensibles correspondent à une catégorie de données personnelles à part, qui nécessite une plus grande vigilance dans leur traitement.

Plus largement, **pensez à structurer la gestion des données par des procédures internes**, et surtout à communiquer sur ces procédures auprès des membres, bénévoles ou salariés. Là encore, la rigueur est de mise. En effet, les menaces, en particulier sur Internet, sont nombreuses. De plus, pensez également à encadrer la collaboration avec vos fournisseurs pour y inclure les normes RGPD qui encadrent ce type de collaboration.

Enfin, gardez à l'esprit que, même si le RGPD n'a pas vocation à sanctionner immédiatement, il s'agit d'une norme sur laquelle la loi s'appuie pour faire respecter l'une des libertés fondamentales des personnes, à savoir le droit à la transparence sur le traitement de leurs données personnelles.

Pour faire respecter cette réglementation, la CNIL est en mesure de mener des opérations de contrôle dans les locaux de l'association ou en ligne. Dans un premier temps, ces évaluations sont destinées à mettre en garde les organisations qui ne se soumettent pas aux obligations en vigueur.

En cas de récidive, n'importe quelle structure s'expose à des sanctions administratives voire pénales. Sur ce point, le milieu associatif est considéré au même titre que les organisations à but lucratif.

Si vous avez le sentiment de ne pas être à la page en ce qui concerne le RGPD, mieux vaut vous y mettre tout de suite ! Vous aurez ainsi le temps d'adapter les processus à vos habitudes de fonctionnement, et vous pourrez ainsi valoriser votre transparence vis-à-vis de vos membres.

À propos de Joinly

Joinly est une solution d'inscription et de paiement en ligne destinée aux associations qui souhaitent simplifier leur gestion. Le service s'appuie sur une plateforme digitale entièrement pensée pour répondre à leurs besoins si spécifiques. Joinly permet donc aux associations de **dématérialiser entièrement leurs processus d'inscription** par le biais de collectes simples à créer, qu'il s'agisse de cotisations ou d'inscriptions à des événements sportifs et festifs.

Côté financement, Joinly propose aux associations de **digitaliser en quelques clics leurs campagnes d'appels aux dons** en permettant une récolte sécurisée de ceux-ci en ligne. **Une manière simple et agréable d'accroître leurs revenus** et de financer leurs projets à venir par les dons de leur communauté.

Joinly propose deux offres à ses utilisateurs : un service sans abonnement avec des fonctionnalités réduites et des frais sur les transactions réalisées en ligne, et un service avec abonnement pour profiter pleinement de toutes les possibilités et des meilleures fonctionnalités de la solution.

Le service, clé en main, est autant plébiscité **pour sa facilité d'utilisation que pour son ergonomie intuitive**. En 2021, les équipes de Joinly souhaitent continuer d'améliorer le quotidien des associations françaises et de **promouvoir le sport associatif à grande échelle**, en facilitant notamment son accès au plus grand nombre.

Alors, **vous nous rejoignez** ?

Avec le parrainage du

MINISTÈRE CHARGÉ DES SPORTS
Liberté
Égalité
Fraternité

Contactez-nous !

joinly.com

hello@joinly.com

Joinly / WeWork
198 Avenue de France
75013 Paris