ASSOCIATIONS : COMMENT APPLIQUER LE RGPD ?

Date de publication : **29/01/2020 - Droit/justice**

Le 25 mai 2018, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après "RGPD") est entré en vigueur. Le RGPD assure une protection des données à caractère personnel (autre terme utilisé : données personnelles) des personnes physiques. Il abroge la directive européenne 95/46/CE sur la protection des données à caractère personnel, qui était en vigueur jusqu'au 24 mai 2018.

La protection des données personnelles est également encadrée en France par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Elle a été modifiée pour s'adapter aux dispositions du RGPD.

1 - Je suis une association. Suis-je concernée ? Dois-je appliquer le RGPD ?

Une donnée personnelle se définit comme toute information qui se rapporte directement ou indirectement à une personne physique (article 4 du RGPD).

Exemple(s) Nom, prénom, date de naissance, numéro de téléphone, adresse mail, adresse postale, adresse IP ...

On parle de traitement de données personnelles lorsqu'une donnée personnelle est manipulée informatiquement ou manuellement par le biais d'opérations telles que la collecte, l'enregistrement, la conservation, la modification, la consultation, la diffusion ou l'effacement (article 4 du RGPD).

Le RGPD a donc un champ d'application très large, car il s'applique dès lors qu'une donnée personnelle, comprise dans un fichier papier ou sur ordinateur, est manipulée.

1 - Je suis une association. Suis-je concernée ? Dois-je appliquer le RGPD ?

OUI
Le RGPD s'applique à tout organisme, quel que soit son statut (privé, public), sa taille, sa forme juridique, ses activités, etc., du moment qu'il traite de données personnelles de personnes résidant dans l'Union européenne.

Une association traite des données personnelles de ses membres, ses salariés, ses bénévoles et ses adhérents (ex. nom, prénom, adresse mail?). Le RGPD s'applique, de ce fait, aux associations.

Le RGPD s'applique :

- au **responsable du traitement**, c'est-à-dire l'association, en tant que personne morale. Car elle détermine les moyens et les finalités du traitement de données personnelles, ET
- au **sous-traitant**, c'est-à-dire l'entreprise ou l'organisme qui va aider l'association dans le traitement des données personnelles (hébergeurs, intégrateurs de logiciels, agences de communication, etc.).

A noter L'association peut également être un sous-traitant si elle sous-traite une activité comportant des données personnelles pour une autre entreprise ou organisme.

2 - Le RGPD s'applique-t-il aussi aux fichiers papier ?

OUI
Le RGPD s'applique aux données personnelles contenues :

- dans des fichiers informatiques (ex. liste des membres, dossiers de litige...),
- dans des fichiers papier (ex. dossiers classés par ordre alphabétique, ...)

Du moment qu'une donnée personnelle est contenue dans un fichier (annuaire, base de données, sur ordinateur ou sur papier, etc.), le RGPD s'applique.

Une donnée personnelle est toute information qui se rapporte directement ou indirectement à une personne physique (article 4 du RGPD). C'est une définition large regroupant une grande quantité de données.

Exemple(s) Nom, prénom, date de naissance, numéro de téléphone personnel ou professionnel, adresse mail personnelle ou professionnelle, adresse postale personnelle ou professionnelle, cookies, adresse IP, identifiant numérique, numéro de carte de paiement, numéro de sécurité sociale, plaque d'immatriculation?

Le RGPD s'applique aux traitements de données personnelles concernant des personnes **résidant dans l'Union européenne.** En pratique, le RGPD s'applique à chaque fois qu'un résident européen, quelle que soit sa nationalité, est directement visé par un traitement de données, y compris par Internet ou par le biais d'objets connectés (ex. enceintes connectées, etc.).

A noter Veillez à respecter le **principe de minimisation des données**. Limitez au maximum la collecte des données personnelles et assurez-vous de ne collecter que les données personnelles strictement nécessaires à l'exercice de votre activité. Ex. il n'est pas nécessaire de demander la date de naissance dans un bulletin de dons.

3 - Combien de temps dois-je conserver les données personnelles ?

Les données personnelles doivent être conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités (c'est-à-dire les objectifs poursuivis) pour lesquelles elles sont traitées. Ex. traiter un dossier de contentieux, envoyer une lettre d'information, etc.

Pour chaque traitement de données personnelles, la question de la durée de conservation doit être envisagée. A noter que le RGPD ne donne pas une liste des traitements avec les durées de conservation.

Ces options peuvent être envisagées :

- Suivre les recommandations de la CNIL : la CNIL avait établi des recommandations sur les durées de conservation (anciennes normes qui n'ont plus de valeur juridique à compter du 25 mai 2018). Il est possible de se référer à ces recommandations, en attendant la production de référentiels RGPD.
- Fixation en interne d'une règle de durée de conservation. L'association doit se poser deux questions :
  1 - Combien de temps dois-je conserver un document lors du traitement de données personnelles ? Exemple : dans le cadre de la relation contractuelle liée à l'adhésion de la personne. Le document sera en **base active**.
  2 - Je ne traite plus les données personnelles (ex. départ d'un adhérent, fin d'abonnement). Toutefois, j'ai besoin des documents à titre de preuves en cas de contentieux, pour respecter des durées de prescriptions légales (ex. durée de prescription de 5 ans en droit commun des contrats, 10 ans en matière comptable)? Le document sera en **archive intermédiaire**. C'est-à-dire qu'il sera dans un dossier verrouillé avec un accès restreint. Et ne pourra pas être utilisé pour d'autres fins.

Les données qui ne sont plus nécessaires à l'exercice de l'activité doivent être supprimées. Elles peuvent être **conservées si les données sont anonymisées**.

Notre conseil Penser à effectuer une purge régulière des données personnelles qui ne sont plus nécessaires à l'exercice de l'activité.

4 - Je traite des données sensibles (certificats médicaux?) Quelles sont les conséquences ?

Les données sensibles sont des données qui révèlent :

- l'origine raciale ou ethnique,
- les opinions politiques,
- les convictions religieuses ou philosophiques ou l'appartenance syndicale,
- le traitement des données génétiques, des données biométriques aux fins d'identifier une personne de manière unique,
- des données concernant la santé,
- des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne.

(article 4, considérant 35 du RGPD).

Est en principe interdit, le traitement des données sensibles, sans le consentement explicite des personnes concernées (article 9 du RGPD, article 6 de la loi "Informatique et Libertés").

Il existe des **exceptions** à l'interdiction de traitement de données sensibles (ex : droit du travail, motifs d'intérêt public important, intérêts vitaux, etc.). Ou bien lorsque l'adhérent a donné explicitement son consentement.

Notre conseil Evitez au maximum de traiter des données sensibles. Si vous êtes amenés à le faire par nécessité (ex. traitement d'un dossier de recouvrement avec des certificats médicaux?), pensez à demander le consentement explicite de l'adhérent lors de son inscription (ex. case à cocher dans un bulletin d'inscription). Sans consentement, il vous sera impossible de traiter de données sensibles (voir la question 5 sur le consentement).

5 - Dois-je demander un consentement à l'adhérent lorsque je traite ses données personnelles ?

PAS TOUJOURS

Le consentement est un des six fondements juridiques permettant de rendre licite un traitement de données personnelles (article 6 du RGPD). Ce qui signifie que la demande d'un consentement n'est pas systématique.

Les données personnelles traitées **qui ne sont pas des données sensibles** peuvent ne pas faire l'objet d'une demande de consentement si elles sont justifiées comme suit :

- traitement nécessaire à l'exécution d'un contrat ou à l'exécution de mesures précontractuelles (ex. adhésion à l'associaion, abonnement au journal...),
- traitement qui répond à une obligation légale,
- traitement nécessaire à la sauvegarde des intérêts vitaux de la personne,
- traitement nécessaire aux fins des intérêts légitimes poursuivis par le responsable de traitement.

Exemple de situation dans laquelle la demande de consentement est obligatoire : lors de l'envoi de la lettre d'information.

Notre conseil Conservez la preuve que le consentement a bien été donné (ex. mail de confirmation). Le consentement doit pouvoir être retiré à tout moment.

Attention Si vous recueillez des données sensibles (voir la question 4 pour la définition des données sensibles), dans tous les cas, il faudra demander un consentement explicite de la personne. Le consentement doit être donné pour chaque finalité spécifique.

Exemple(s) Un adhérent s'engage dans votre association. Il est susceptible de vous fournir un certificat médical. Il s'agit d'un document contenant des données sensibles. Pour être conforme au RGPD, pensez à demander le consentement par le biais d'une case à cocher.

Exemple(s) de formulation " Je consens à ce que l'association X traite mes données sensibles dans le cadre de la gestion de mes dossiers de précontentieux".

6 - Dois-je désigner un Délégué à la Protection (DPO / DPD) ?

PAS DE MANIERE AUTOMATIQUE
La désignation d'un Délégué à la Protection des Données (DPD) (aussi appelé "DPO" - Data Protection Officer) n'est pas obligatoire pour une association.

Toutefois, la désignation devient **obligatoire** lorsque l'association traite :

- des données sensibles (ex. certificat médical, numéro de sécurité sociale ?) à grande échelle ;
- des données personnelles exigeant un suivi régulier et systématique à grande échelle de personnes (ex. profilage ?) (article 37.1 du RGPD).

Le Délégué à la Protection des Données a pour mission de :

- informer et conseiller le responsable de traitement (c'est-à-dire l'association qui met en ?uvre les traitements des données personnelles) ainsi que l'ensemble du personnel. Mais aussi les sous-traitants (c'est-à-dire les entreprises ou organismes qui vont aider l'association dans le traitement des données personnelles (hébergeurs, intégrateurs de logiciels, agences de communication, etc.),
- contrôler le respect du RGPD et de la législation nationale,
- conseiller l'association sur tout sujet relatif à la protection des données personnelles (ex. comment mettre en place un formulaire avec des mentions RGPD),
- coopérer avec l'autorité de contrôle (c'est-à-dire la CNIL). Il s'agit de l'organisme chargé de conseiller les entreprises et organismes dans la mise en place du RGPD. Il a aussi un pouvoir de contrôle et de sanctions. Cliquez ici pour en savoir plus sur les missions de la CNIL.

Le Délégué à la Protection des Données peut être désigné en interne (ex. salarié ayant des compétences informatiques et/ou juridiques) ou bien un prestataire externe (ex. cabinet d'avocats?).

7 - Dois-je répertorier toutes les données personnelles que je traite dans un registre des traitements ?

PAS OBLIGATOIRE, MAIS RECOMMANDE
En principe, une association comportant moins de 250 salariés n'a pas à répertorier toutes les données personnelles traitées, sous forme de registres des traitements.

Toutefois, cela devient une obligation si l'association effectue des traitements :

- susceptibles de comporter un risque pour les droits et les libertés des personnes (ex. traitement d'un dossier comportant des fichiers de nature médicale?) et de manière non occasionnelle,
- portant sur des données sensibles ou des condamnations et infractions pénales (voir la question 4 pour la définition des données sensibles).

Néanmoins, il est recommandé de tenir un registre des traitements. Le recensement des différents traitements de données personnelles traitées, des durées de conservation, des modes d'archivage, etc. vous sera utile pour mieux vous organiser en interne. En mettant par exemple en place des process ou encore en cas de contrôle de la CNIL.

La CNIL propose sur son site internet un modèle de registre des traitements, pouvant être téléchargé pour être complété (fichier en format Excel).

Les informations devant figurer dans le registre :

- noms et coordonnées du responsable de traitement et DPO,
- finalités du traitement (objectifs poursuivis),
- description des catégories de personnes concernées et des catégories de données personnelles,
- catégories de destinataires,
- délais prévus pour l'effacement,
- description générale des mesures de sécurité techniques et organisationnelles.

---

8 -Dois-je informer les adhérents du traitement de leurs données personnelles ?

OUI

L'adhérent doit être informé du traitement de ses données personnelles, **par exemple** :

- au moment de son adhésion (formulaire d'inscription),
- au moment de s'inscrire à la lettre d'information (par internet),
- en consultant le site internet de l'association (politique de protection des données),
- au moment de remplir une feuille de présence pour participer à une formation ou à une réunion (feuille de présence),
- en s'abonnant / effectuant un don (bulletins de dons et d'abonnements).

Les informations devant obligatoirement figurer sont :

- les coordonnées de l'association responsable de traitement,
- les catégories de données personnelles traitées,
- l'origine de la collecte (fichiers interne ou obtenu par une source externe),
- la base légale du traitement (ex. contrat, consentement, ?),
- le caractère obligatoire ou non du traitement,
- les finalités (ex. gérer un dossier, recevoir la newsletter, ?),
- les destinataires (ex. branches d'associations régionales, partenaires, ?),
- les durées de conservation,
- les transferts en dehors de l'Union européenne,
- l'exercice des droits (voir la question 9 sur l'exercice des droits).

Le site de la CNIL donne un exemple de mentions d'informations.

Bon à savoir Si votre association dispose d'un site Internet, il est recommandé d'y faire figurer une politique de protection des données personnelles. Ce document reprend l'ensemble des informations ci-dessus.

9 - Comment gérer l'exercice des droits des personnes ?

Les associations doivent répondre aux personnes qui souhaitent exercer leurs droits sur leurs données personnelles.

Les personnes, dont les données personnelles sont traitées, ont un droit :

- à l'information,
- d'accès,
- de rectification (ex. changement d'adresse),
- d'opposition,
- à la portabilité,
- à la limitation du traitement,
- d'effacement,
- de définir des directives relatives au sort de leurs données personnelles après leur mort.

Lorsqu'une personne exerce ses droits (ex. réception d'une demande de droit d'accès ou de suppression), l'association doit lui répondre dans un délai d'**un mois** à compter de la réception de la demande. L'envoi des documents, pour l'exercice du droit d'accès, est en principe **gratuit** (sauf caractère répétitif des demandes).

Si une réponse ne peut être apportée au demandeur, l'association doit obligatoirement indiquer les **motifs du refus** ainsi qu'indiquer la possibilité d'introduire une réclamation auprès de la CNIL et de former un recours juridictionnel.

La gestion des demandes d'exercice des droits nécessite de mettre en place des procédures internes.

10 - Quelles mesures de sécurité dois-je mettre en place ?

Le RGPD indique qu'il faut une obligation renforcée de la sécurisation des données personnelles.

Il existe en effet des risques en matière de cybersécurité :

- motivations financières, espionnage, revendications politiques, déstabilisation, vandalisme?
- usurpation d'identité, escroquerie, abus de confiance, chantage, vengeance, fraude?
- attaques informatiques ciblées (ex. attaques dans les pièces jointes, lien dans un mail frauduleux?),
- virus, hameçonnage, cheval de troie?

La sécurisation des fichiers papier et informatique doit être **organisationnelle** et **matérielle** : gestion des accès aux fichiers protégés, accès par personnes habilitées, mots de passe très sécurisés, sécurisation des réseaux, etc. (article 32 du RGPD).

L'association a également une obligation de **notification à la CNIL de failles de sécurité** (ex. piratage informatique), dans les meilleurs délais, et si possible dans les 72 h, au plus tard après en avoir pris connaissance (article 33 du RGPD). De plus, si la faille de sécurité comporte des **risques pour les droits et libertés des personnes physiques** (ex. partage de numéros de sécurité sociale risquant d'entraîner des cas d'usurpation d'identité), l'association devra également **en notifier les personnes concernées**, dans les meilleurs délais (article 34 du RGPD).

En outre, le RGPD encadre strictement **les transferts de données hors Union européenne (UE).** L'association doit éviter, si besoin, de transférer des données personnelles hors de l'UE. Si l'association travaille avec des entreprises qui sous-traitent des données en dehors de l'UE, des garanties juridiques devront être mises en place (ex. clauses contractuelles types de protection?).

11 - J'envoie des lettres d'information. Que dois-je mettre en place pour être en conformité ?

L'association doit informer les personnes du traitement de leurs données personnelles et demander leur consentement.

Lors de l'inscription, l'adhérent doit être informé clairement de l'utilisation qui sera faite de ses données. L'association doit faire figurer, par exemple sur son site Internet, les informations suivantes :

- les catégories de données personnelles traitées,
- l'origine de la collecte (fichier interne ou obtenu par une source externe),
- la base légale du traitement (ex. contrat, consentement?),
- le caractère obligatoire ou non du traitement,
- les finalités (ex. recevoir la newsletter?)
- les destinataires (ex. branches d'associations régionales, partenaires?),
- les durées de conservation,
- les transferts en dehors de l'Union européenne,
- l'exercice des droits (voir question 8 sur l'exercice des droits),
- la sécurisation des données.

Le site de la CNIL donne un exemple de mentions d'informations.

En outre, l'association doit demander le consentement de l'utilisateur pour l'envoi de courriels. Cela peut se matérialiser par une case à cocher au moment de renseigner l'adresse mail.

A noter que l'adhérent doit avoir la possibilité de se désinscrire, à tout moment de la lettre d'information, en retirant son consentement. Par exemple en cliquant sur un lien de désabonnement ou en envoyant un mail.

Notre conseil Conservez la preuve que le consentement a bien été donné (ex. mail de confirmation). Le consentement doit pouvoir être retiré à tout moment.

Attention **Ces informations essentielles ne préjugent pas des règles appliquées par vos instances nationales et fédérations. Référez-vous à ces dernières pour toute question concernant l'application du RGPD.**

TEXTES DE LOIS
> Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
> Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

En savoir plus
> La fiche pratique INC "RGPD" : quelle protection pour vos données personnelles ?"
> L'article "Loi Informatique et Libertés : adaptation de la loi au Règlement Général sur la Protection des Données (RGPD)" "

Samia M'HAMDI
Juriste à l'Institut national de la consommation
