# RGPD et associations
# Foire aux questions

Si le Règlement général sur la protection des données (RGPD) s'inscrit sur certains points dans la continuité des textes existants, puisqu'il confirme des principes et préceptes existants tels que la transparence, la licéité, la proportionnalité, la sécurisation et les obligations de fond de la loi "Informatique et Libertés", il impose toutefois aux organismes une plus grande responsabilisation. Entré en vigueur le 25 mai, le RGPD conduit ainsi les associations à devoir formaliser leur réflexion sur les données qu'elles collectent et ce qu'elles en font.

Comme a pu le rappeler la Présidente de la CNIL à plusieurs reprises, cette date n'est pas un couperet, mais une réflexion en interne doit être menée au sein de chaque association. Pour ce faire, le Mouvement associatif communique cette foire aux questions qui fait suite à la réunion d'information organisée le 17 mai 2018.

Cette foire aux questions s'appuie sur les réponses qui ont pu être apportées par les intervenants de la réunion du 17 mai, sur les informations disponibles sur le site de la CNIL, ainsi que sur le guide Verticalsoft publié en janvier 2018 et disponible ici. La présente Foire aux questions se veut généraliste et n'est en aucun cas exhaustive, en fonction des particularités sectorielles ou organisationnelles, nous vous invitons à joindre la CNIL. Nous vous informons à ce propos en fin de document des questions que nous avons posées à la CNIL et pour lesquelles nous attendons une réponse qui actualisera, le cas échéant, le présent document.

**Les associations sont-elles concernées par le RGPD ?**

Sur son site ; la CNIL le rappelle :

« Oui, les associations devront également respecter le Règlement européen sur la protection des données à partir du 25 mai 2018.
Si elles collectent, stockent, utilisent des données à caractère personnel. Dans ce cas, les associations sont "responsable de traitement".
Si elles traitent des données à caractère personnel pour le compte d'autres personnes morales. Dans ce cas, les associations sont "sous-traitantes". »

➔ **NOTIONS CLEFS DE LA RGPD**

**Qu'est-ce qu'une donnée à caractère personnel ?**

**Qu'est-ce qu'un traitement ?**

**Dois-je constituer un registre des traitements ?**

**Doit-on fixer des durées de conservation des fichiers de données personnelles**

**Qui est le responsable du traitement ?**

**Qu'est-ce qu'un sous-traitant ?**

**Désigner un délégué à la protection des données, est-ce obligatoire ?**

➔ **EN PRATIQUE POUR LES ASSOCIATIONS**

**Se mettre en conformité, qu'est-ce que cela signifie pour une association ?**

**Quelles sont les actions principales à mener pour entamer votre mise en conformité aux règles de protection des données ? cf. guide CNIL/BPI pour les TPE/PME**

**Où puis je me procurer un modèle de registre de traitement ?**

**Quid du maintien de la dispense de déclaration pour leurs membres et donateurs dont bénéficiaient les associations non lucratives dans le cadre de la RGPD ?**

**Dois-je obtenir le consentement pour l'utilisation des données de mes membres, donateurs ou partenaires ?**

**Dans la pratique votre association a des listes mails pour sa newsletter par exemple, doit-elle demander le consentement pour l'utilisation de ces données dans le cadre des activités de l'association ?**

**Comment obtenir les consentements explicites ?**

**Doit-on mentionner au registre des traitement les fichiers constitués pour des réunions ou événements ponctuels ?**

**L'activité de profilage (cas des associations faisant appel au don) est-elle encore possible dans le cadre du RGPD ?**

**Un maire peut-il exiger la liste des membres ou bénéficiaires d'une association qu'il subventionne ?**

## NOTIONS CLEFS DE LA RGPD

### Qu'est-ce qu'une donnée à caractère personnel ?

Constitue une donnée à caractère personnel toute information se rapportant à une personne physique identifiée ou identifiable directement ou indirectement, notamment par référence à un identifiant (tel qu'un nom, une donnée de localisation etc.), à un ou plusieurs éléments spécifiques propres à son identité (psychique, économique, culturelle, sociale etc.). Ainsi cela inclut les informations sur les membres, les volontaires, les donateurs, les employés, les partenaires etc.

*Exemple :*
*Les noms, prénoms, adresse mails, adresses postales, qui peuvent figurer sur vos fichiers de type Excel, les bulletins d'adhésion, les contrats de travail, etc. sont des données à caractère personnel.*

*Cependant, une donnée qui ne vise pas directement (ou indirectement) une personne physique tel que par exemple, le nom d'une association « Les amis de A » avec son adresse postale, le numéro de téléphone de son standard et un email de contact générique « associationA@email.fr », ne constitue pas une donnée à caractère personnel.*

### Qu'est-ce qu'un traitement ?

Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou un ensemble de données à caractère personnel, telles que : la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, la consultation, l'utilisation, l'extraction, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

### Dois-je constituer un registre des traitements ?

Le RGPD prévoit certains cas pour lesquels la tenue d'un registre des traitements est obligatoire. Toutefois, dès lors que vous traitez des données personnelles (voir définition ci-dessus), il est fortement recommandé de tenir un registre des traitements.

### Doit-on fixer des durées de conservation des fichiers de données personnelles ?

Oui.

Vous ne pouvez pas conserver indéfiniment des informations sur des personnes physiques dans vos fichiers.

Si une durée de conservation n'est pas imposée par un texte légal (par exemple, 10 ans pour les documents comptables), il vous appartient de fixer vous-même cette durée en fonction de l'utilité de la donnée au regard du but poursuivi.

Attention : la durée de conservation des données que vous fixerez ne devra pas être excessive au regard des raisons pour lesquelles vous les avez collectées (par exemple, le temps de la relation contractuelle pour les informations figurant dans un fichier clients).

Au-delà de cette durée, vous devez effacer ou anonymiser les données.

A savoir : si vous déclarez vous conformer à une norme fixée par la CNIL, ce texte vous précisera toujours la durée de conservation qui s'applique aux données que vous pouvez collecter et traiter (par exemple, 2 mois pour les données relatives à géolocalisation d'un véhicule utilisé par un employé).

## Qui est le responsable du traitement ?

Le responsable d'un traitement de données à caractère personnel est en principe la personne, l'autorité publique, la société ou l'organisme qui détermine les finalités et les moyens de ce fichier, qui décide de sa création. En pratique, il s'agit généralement de la personne morale (entreprise, collectivité, etc.) incarnée par son représentant légal (président, maire, etc.).

## Qu’est-ce qu’un sous-traitant ?

C’est une personne physique ou morale, service, autorité publique ou autre organisme, qui traite des données à caractère personnel pour le compte du responsable de traitement. Cela est par exemple le cas des sociétés d’informatiques avec leur association cliente.

## Désigner un délégué à la protection des données, est-ce obligatoire ?

La désignation d'un Délégué sera obligatoire pour les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle. Par exemple : les compagnies d'assurance ou les banques pour leurs fichiers clients, les opérateurs téléphoniques ou les fournisseurs d'accès internet.
Les organismes dont les activités de base les amènent à traiter à grande échelle des données dites "sensibles" (données biométriques, génétiques, relatives à la santé, la vie sexuelle, l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale) ou relatives à des condamnations pénales et infractions.

## EN PRATIQUE POUR LES ASSOCIATIONS

### Se mettre en conformité, qu'est-ce que cela signifie pour une association ?

La mise en conformité RGPD est essentiellement organisationnelle : c'est la mise en place d'outils et de bonnes pratiques au sein de votre association. Plusieurs actions peuvent être recommandées (voir question suivante).

### Quelles sont les actions principales à mener pour entamer votre mise en conformité aux règles de protection des données ? cf. guide CNIL/BPI pour les TPE/PME

#### ACTION 1 DESIGNEZ UN PILOTE AU SEIN DE VOTRE ORGANISATION

#### ACTION 2 - RECENSEZ VOS FICHIERS

Faire un registre listant vos traitements de données vous permettra d'avoir une vision d'ensemble. Identifiez les activités principales de votre association qui nécessitent la collecte et le traitement de données (exemples : recrutement, gestion de la paye, formation, gestion des donateurs, enquêtes statistiques etc.).

Appuyez-vous sur le modèle de registre proposé par la CNIL sur son site internet à télécharger ici.

Dans votre registre, créez une fiche pour chaque activité recensée, en précisant :

• l'objectif poursuivi (la finalité - exemple : la fidélisation client) ;

• les catégories de données utilisées (exemple pour la paie : nom, prénom, date de naissance, salaire, etc.) ;

• qui a accès aux données (le destinataire - exemple : service chargé du recrutement, service informatique, direction, prestataires, partenaires, hébergeurs) ;

• la durée de conservation de ces données (durée durant laquelle les données sont utiles d'un point de vue opérationnel, et durée de conservation en archive).

Le registre est placé sous la responsabilité du Président.

Pour avoir un registre exhaustif et à jour, il faut en discuter et être en contact avec toutes les personnes de l'association susceptibles de traiter des données personnelles.

En constituant votre registre, vous aurez une vision d'ensemble sur vos traitements de données.

**ACTION 3 FAITES LE TRI DANS VOS DONNEES**

Pour chaque fiche de registre créée, vérifiez :

• que les données que vous traitez sont nécessaires à vos activités (par exemple, il n'est pas utile de savoir si les salariés de l'association ont des enfants, si l'association n'offre aucun service ou rémunération attachée à cette caractéristique) ;

• que vous ne traitez aucune donnée dite « sensible » ou, si c'est le cas, que vous avez bien le droit de les traiter ;

• que seules les personnes habilitées ont accès aux données dont elles ont besoin ;

• que vous ne conservez pas vos données au-delà de ce qui est nécessaire.

À cette occasion, améliorez vos pratiques ! Minimisez la collecte de données, en éliminant de vos formulaires de collecte et vos bases de données toutes les informations inutiles. Redéfinissez qui doit pouvoir accéder à quelles données dans votre association. Pensez à poser des règles automatiques d'effacement ou d'archivage au bout d'une certaine durée dans vos applications.

**ACTION 4 RESPECTEZ LES DROITS DES PERSONNES**

À chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information.

Vérifiez que l'information comporte notamment les éléments suivants :

• pourquoi vous collectez les données (« la finalité » ; par exemple pour gérer l'achat en ligne du consommateur) ;

• ce qui vous autorise à traiter ces données (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 vous les conservez (exemple : « 5 ans après la fin de la relation contractuelle ») ;

• 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 vous transférez des 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. Pour éviter des mentions trop longues au niveau d'un formulaire en ligne, vous pouvez par exemple, donner un premier niveau d'information en fin de formulaire et renvoyer à une politique de confidentialité/ page vie privée sur votre site internet. À l'issue de cette étape, vous avez répondu à votre obligation de transparence.

**ACTION 5 SECURISEZ VOS DONNEES**

Vous êtes en effet tenu d'assurer la sécurité des données personnelles que vous détenez. Garantissez l'intégrité de votre patrimoine de données en minimisant les risques de pertes de données ou de piratage.

Les mesures à prendre, informatiques ou physiques, dépendent de la sensibilité des données que vous traitez et des risques qui pèsent sur les personnes en cas d'incident.

Différentes actions doivent être mises en place : 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. En cas de perte ou vol d'un outil informatique, il sera plus difficile pour un tiers d'y accéder.

**Où puis je me procurer un modèle de registre de traitement ?**

Sur le site de la CNIL, à télécharger ici.

**Quid du maintien de la dispense de déclaration pour les membres et donateurs dont bénéficiaient les associations non lucratives dans le cadre de la RGPD ?**

Les fichiers des membres, bénévoles et donateurs d'associations étaient auparavant dispensés de déclaration auprès de la CNIL dès lors qu'ils respectaient les conditions posées par la CNIL. Dans le cas contraire, ces fichiers devaient faire l'objet d'une déclaration normale.

**La dispense de déclaration n'impliquait qu'une dispense de réalisation des formalités auprès de la CNIL. L'association devait tout de même respecter les obligations de fond de la loi "Informatique et Libertés".**

Le RGPD inverse la tendance en supprimant les obligations déclaratives auprès de la CNIL et en responsabilisant les organismes qui doivent se mettre en conformité avec le RGPD.

La mise en conformité avec le RGPD se fait par la mise en place d'outils tels que notamment la tenue d'un registre des traitements, le cas échéant, la désignation d'un délégué à la protection des données (DPO etc.).

**Dois-je obtenir le consentement pour l'utilisation des données de mes membres, donateurs ou partenaires ?**

Non, le consentement de la personne dont les données sont enregistrées dans un fichier n'est pas nécessaire lorsque ces données sont collectées dans le cadre de l'exécution d'un contrat, du respect d'une obligation légale, d'une mission d'intérêt public ou **de votre intérêt légitime**.

En dehors de ces cas, le consentement de la personne concernée est obligatoire, **il doit être explicite.** C'est le consentement qui confère alors au fichier projeté son caractère licite.

**Dans la pratique votre association a des listes mails pour sa newsletter par exemple, doit-elle demander le consentement pour l'utilisation de ces données dans le cadre des activités de l'association ?**

Le consentement n'est pas toujours nécessaire mais il reste un moyen sûr pour légitimer l'utilisation des données.

Le cas échéant l'association doit s'assurer du consentement explicite des personnes inscrites sur la mailing list pour l'utilisation de leurs données. Le silence n'est pas un consentement. Une case pré-cochée n'est pas un consentement. Aussi, à titre d'exemple, si l'association envoie à la mailing list newsletter un mail pour s'assurer du consentement des utilisateurs, pour lequel seuls 20% des utilisateurs envoient leur consentement, et 80% ne font aucun retour, doit-elle considérer qu'elle n'obtient pas le consentement pour l'utilisation des données de 80% de ses utilisateurs. Il conviendra dès lors de les sortir du fichier.

**Comment obtenir les consentements explicites ?**

Nous reprenons ici une recommandation du guide Verticalsoft de janvier 2018 disponible en ligne.

**Rédigez un texte de demande de consentement**. Par exemple

« *En faisant ce don (en remplissant ce formulaire etc.), vous acceptez que l'Association XYZ mémorise et utilise vos données personnelles collectées dans ce formulaire dans le but d'améliorer votre expérience et vos interactions avec elle. En l'occurrence, vous autorisez l'Association XYZ à communiquer occasionnellement avec vous si elle le juge nécessaire afin de vous apporter des informations complémentaires sur ses projets et appels à dons via les coordonnées collectées dans le formulaire.*

*Afin de protéger la confidentialité de vos données personnelles, l'Association XYZ s'engage à ne pas divulguer, ne pas transmettre, ni partager vos données personnelles avec d'autres entités, entreprises ou organismes, quels qu'ils soient, conformément au Règlement Général de Protection des Données de 2018 sur la protection des données personnelles et à notre politique de protection des données* »

**Demandez clairement et activement le consentement sur vos formulaires.** Ajoutez une case vide que l'utilisateur devra cocher afin de démontrer qu'il a donné son consentement explicite.

**Pour aller plus loin, vous pouvez ajouter un mécanisme de « double Opt-in » afin de prouver le consentement explicite de vos contacts.** Le « double Opt-in » consiste à demander une confirmation par courriel à chaque personne concernée qui a rempli un formulaire sur votre site web. Afin de valider leur consentement, ils devront alors cliquer sur un lien dans un courriel de confirmation.

Il est important de conserver les preuves de consentement dans un dossier.

## Doit-on mentionner au registre des traitements les fichiers constitués pour des réunions ou événements ponctuels ?

Le guide CNIL/BPI pour les TPE/PME mentionne qu'il n'y a pas lieu d'inscrire au registre des traitements les traitements purement occasionnels. Cela concerne donc les fichiers de noms constitués en vue d'un événement ponctuel ou d'une réunion ou d'une campagne de communication. Attention cette tolérance ne s'applique qu'aux associations de moins de 250 salariés.

## L'activité de profilage (cas des associations faisant appel au don) est-elle encore possible dans le cadre du RGPD ?

Le RGPD n'interdit pas le profilage, il indique qu'un traitement de ce type doit être assorti de garanties appropriées. La CNIL indique « avec le RGPD, l'information des personnes est renforcée. Le responsable du fichier doit être transparent avec les personnes dont il traite les données. (…) Ainsi, les personnes doivent être informées (…) De l'existence d'une prise de décision automatisée ou d'un profilage, des informations utiles à la compréhension de l'algorithme et de sa logique, ainsi que des conséquences pour la personne concernée ».

## Un maire peut-il exiger la liste des membres ou bénéficiaires d'une association qu'il subventionne ?

Non.

En vertu du principe de liberté d'association, une collectivité (mairie, conseil départemental, etc.) ne peut pas demander à une association la liste nominative de ses adhérents. Seule la transmission de données statistiques anonymes est admise.

Pour contrôler les subventions versées à une association, les collectivités peuvent lui demander la copie certifiée de son budget et de ses comptes annuels, son rapport annuel et tous les documents concernant son activité.

❖

Enfin le Mouvement associatif a adressé les questions suivantes à la CNIL à l'issue de la réunion d'information du 17 mai 2018, et actualisera la présente foire aux questions en fonction des retours de la CNIL.

**Un bénévole peut-il être désigné référent ou délégué à la protection des données (DPO) ? (Cas notamment des associations ne comptant aucun salarié)**

**Les fichiers d'adhérents qui sont conservées pendant plusieurs années et qui peuvent servir à mesurer l'impact d'une action associative sur du long terme (réunion d'anciens volontaires, bénévoles du type « que sont-ils devenus ? » etc.) peuvent-ils être conservés plus de 10 ans eu égard de leur objectif ?**

**Les fédérations qui hébergent des pages internet pour leurs membres qui se chargent eux-mêmes de mettre le contenu sur leurs pages, sont-elles responsables des données qui y sont mises ?**