GUIDE FSGT POUR
LA SENSIBILISATION SUR LE

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

SOMMAIRE

Avant propos 3

I - LES NOTIONS DE LA PROTECTION DES DONNÉES 4
- Qu'est-ce qu'une donnée personnelle ? 4
- Qu'est-ce qu'un traitement (ou fichier) de données personnelles ? 4
- Qu'est-ce qu'une finalité ? 5
- Qu'est-ce qu'une donnée sensible ? 5
- Qu'est-ce qu'un responsable de traitement ? 6
- Qu'est-ce qu'un destinataire ? 6
- Qu'est-ce qu'un tiers autorisé ? 6
- Qu'est-ce qu'un sous-traitant ? 6

II - LES GRANDS PRINCIPES À RESPECTER 7
- Principe de Licéité 7
- Principe de Finalité déterminée & légitime 7
- Principe de Pertinence & de minimisation 7
- Principe de Transparence & de respect des droits des personnes 8
- Principe de Durée de conservation limitée 8
- Principe de Confidentialité & de sécurité 9

III - LES PREMIÈRES ÉTAPES DE LA MISE EN CONFORMITÉ 10
- Recenser les fichiers 10
- Faire le tri dans les données 10
- Faire preuve de transparence 11
- Organiser & faciliter l'exercice des droits des personnes 11
- Sécuriser les données 11

IV - DES ÉLÉMENTS À UTILISER POUR ÊTRE EN CONFORMITÉ AU RGPD 13
- Modèle de texte 13
- Clauses RGPD entre un responsable de traitement et un sous-traitant 13

AVANT PROPOS

La France dispose d'un tissu associatif particulièrement riche, recensant plus de 1,3 million d'associations aux profils divers tant en termes de taille que de secteurs d'activité (caritatif, politique, sportif, social, etc.).
Concentrées sur leurs missions, certaines structures ne disposent pas toujours de ressources dédiées spécifiquement à la protection des données. Pourtant, la plupart d'entre elles collectent de nombreuses informations sur les personnes dans le cadre de leurs activités.
Quelle que soit la taille de la structure, les risques d'atteinte à la vie privée des personnes concernées (usagers, adhérents, bénéficiaires, etc.) peuvent être importants en cas de divulgation d'informations personnelles à des tiers. Il est donc essentiel que ces associations préservent les droits et libertés des personnes concernées.

Qu'est-ce-que le Règlement Général sur la Protection des Données (RGPD) ?

Comme son nom l'indique le RGPD est un Règlement qui vise à protéger les droits des personnes par rapport au traitement de leurs données, il est adopté par le Parlement européen et du Conseil de l'U.E le 27 avril 2016 et il est entré en vigueur le 25 mai 2018.
La protection des données physiques à l'égard du traitement des données à caractère personnel est un droit fondamental.

Quelles sont les obligations des associations en matière de protection des données ?

Le RGPD reprend les grands principes déjà présents depuis le 6 janvier 1978 dans la loi Informatique fichiers et Libertés.
Le texte abandonne la logique basée sur les déclarations à adresser à la Commission Nationale de l'Informatique et des Libertés (CNIL) pour privilégier une logique de responsabilisation des acteurs utilisant des données personnelles : les associations n'ont donc plus à déclarer leurs fichiers à la CNIL avant leur mise en œuvre (sauf exceptions dans le domaine de la santé).
En contrepartie, les organismes doivent s'assurer que leurs fichiers et services numériques sont, en permanence, conformes au RGPD. Cela nécessite de tenir à jour une documentation des actions menées afin de pouvoir démontrer le respect des règles et notamment :

- Recenser les fichiers (traitements) et tenir à jour le registre les détaillant
- Encadrer la sous-traitance des traitements
- Garantir la sécurité des données
- Organiser la réponse aux demandes d'exercice des droits venant des personnes dont les données personnelles sont traitées
- Informer la CNIL, voire les personnes concernées, des violations éventuelles de sécurité de données personnelles (par exemple la perte de document ou les failles de sécurité)
- Effectuer dans certains cas des analyses d'impact sur la vie privée (AIPD) pour certains fichiers à risques

Focus sur le délégué à la protection des données (DPD ou DPO)

La désignation d'un référent ou d'un DPD/DPO (Data Protection Officier), chargé de piloter les démarches de mise en conformité au RGPD n'est pas obligatoire pour les associations, sauf dans certains cas (une association du secteur social et médico-social devra a priori désigner un DPO dans la mesure où elle traite des données sensibles à grande échelle). Pour autant, afin de consolider les relations de confiance avec les personnes concernées par leurs traitements, et limiter les risques juridiques et d'image liés à une mauvaise utilisation des fichiers, les associations ont tout intérêt à se doter d'une telle fonction (le DPO peut être interne, externe ou mutualisé) ou à confier à une personne la mission de veiller au bon respect par la structure des règles applicables en la matière.

Quelles sont les missions de la CNIL ?

La CNIL est l'autorité française de protection des données. Elle poursuit quatre principales missions :

INFORMER & PROTÉGER LES DROITS

La CNIL répond aux demandes des particuliers et des professionnels. Elle mène des actions de communication auprès du grand public et des professionnels que ce soit à travers ses réseaux, la presse, son site web, sa présence sur les réseaux sociaux ou en mettant à disposition des outils pédagogiques. Toute personne peut s'adresser à la CNIL en cas de difficulté dans l'exercice de ses droits.

ANTICIPER & INNOVER

Pour détecter et analyser les technologies ou les nouveaux usages pouvant avoir des impacts importants sur la vie privée, la CNIL assure une veille dédiée. Elle contribue au développement de solutions technologiques protectrices de la vie privée en conseillant les entreprises le plus en amont possible, dans une logique de *privacy by design* (protection dès la conception).

ACCOMPAGNER LA CONFORMITÉ & CONSEILLER

Afin d'aider les organismes privés et publics à respecter le RGPD, la CNIL propose une boîte à outils complète et adaptée en fonction de leur taille et de leurs besoins. La CNIL veille à la recherche de solutions leur permettant de poursuivre leurs objectifs légitimes dans le strict respect des droits et libertés des citoyens.

CONTRÔLER & SANCTIONNER

Le contrôle permet à la CNIL de vérifier la mise en œuvre concrète de la loi. Elle peut imposer à un acteur de régulariser son fichier (mise en demeure) ou prononcer des sanctions (amende, etc.).

I - LES NOTIONS DE LA PROTECTION DES DONNÉES

Qu'est-ce qu'une donnée personnelle ?

Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable.

Une personne physique peut être identifiée :

- Directement (par exemple, nom et prénom)
- Indirectement (par exemple, un numéro d'adhérent, un numéro de téléphone ou de plaque d'immatriculation, le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou la photo d'une personne)

⚠ L'identification d'une personne physique peut être réalisée par un croisement d'un ensemble de données.

EXEMPLES

- Une enquête par questionnaire auprès des adhérents d'une association sportive peut, même lorsque les noms et prénoms ne sont pas indiqués, contenir des réponses qui peuvent permettre de retrouver l'identité des personnes lorsqu'elles sont combinées les unes avec les autres
- La collecte des informations relative à l'âge, au sexe, à la pratique d'un sport à tel niveau au sein de telle ville est susceptible de révéler l'identité de la personne

En revanche, des coordonnées d'associations ou d'entreprises, par exemple, l'association « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un courriel de contact générique, ne sont pas des données personnelles.

Qu'est-ce qu'un traitement (ou fichier) de données personnelles ?

Un traitement de données personnelles est toute manipulation ou utilisation de données personnelles, notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la consultation, l'utilisation, la communication par transmission ou diffusion ou toute autre forme de mise à disposition, le rapprochement, etc.
Cette notion est donc très large : tout maniement de données, y compris une simple consultation, est un « traitement de données personnelles ».

EXEMPLES

- L'installation d'un système de vidéosurveillance ou de vidéoprotection à des fins de sécurité des personnes et des biens au sein de l'association
- Un tableur (Excel, Calc, etc.) qui regroupe l'ensemble des actions effectuées pour aider des usagers
- Le formulaire d'adhésion à l'association
- Une base de données qui regroupe l'ensemble des informations relatives aux usagers
- Etc

⚠ Un fichier ou traitement de données personnelles n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

Qu'est-ce qu'une finalité ?

Un traitement de données poursuit toujours un objectif : c'est sa « finalité ». Celle-ci doit être déterminée, explicite et légitime préalablement au recueil des données et à leur utilisation. Autrement dit, il n'est pas permis de collecter des données si l'on ne sait pas avant quel usage on va en faire.

EXEMPLES

- La gestion administrative des licenciés au sein d'une association sportive
- La gestion administrative des donateurs au sein d'une association caritative
- L'accompagnement et le suivi social des personnes en difficulté au sein d'associations à caractère social
- La tenue d'un annuaire des anciens membres d'une association
- La réalisation par tout moyen de communication des opérations relatives à des actions de prospection caritative/politique/commerciale auprès des membres, adhérents, donateurs, prospects
- Etc

L'objectif doit être respecté : vous ne pouvez pas utiliser votre fichier pour un autre but que celui qui a été fixé. Par exemple, vous ne pouvez pas réutiliser le fichier de recrutement des candidatures à un poste de bénévole et/ou salarié pour proposer des offres commerciales/caritatives concernant votre association aux candidats.

Qu'est-ce qu'une donnée sensible ?

Les données sensibles sont celles qui concernent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale. Elles comprennent également les données génétiques, les données biométriques, les données concernant la santé et les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.
L'utilisation de ces données est, par principe, interdit sauf dans des cas limitatifs prévus par l'article 9.2. du RGPD.

Parmi ces exceptions, on retrouve :

- Le consentement explicite de la personne concernée
- Le fait que les conditions suivantes soient réunies :

  - Le fichier est mis en place par une fondation, une association ou tout autre organisme à but non lucratif
  - L'association poursuit un objectif politique, philosophique, religieux ou syndical
  - Le fichier se rapporte exclusivement aux membres ou aux anciens membres de cet organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités
  - Ces données ne sont pas communiquées en dehors de cet organisme sans l'accord des personnes concernées

EXEMPLES

- Une association organisant des sorties extra-scolaires peut collecter des informations relatives à la santé des enfants (par exemple, allergie, etc.) après recueil de l'accord du représentant légal
- Un parti politique peut recueillir les opinions politiques de ses membres ou des personnes avec lesquels il entretient des contacts réguliers en liaison avec ses missions sous réserve que celles-ci ne soient pas communiquées en dehors de cet organisme (sauf si la personne concernée a donné son accord à cette communication)

Qu'est-ce qu'un responsable de traitement ?

La personne ou l'organisme qui définit les objectifs poursuivis par un traitement et ses modalités pratiques (informations collectées par exemple) est appelé responsable de traitement.

C'est lui qui doit s'assurer que le fichier qu'il met en œuvre respecte les règles. Le responsable de traitement est en général incarné par le représentant légal de la structure.

EXEMPLES

- Le président de l'association caritative
- Le directeur général de la structure sportive
- Etc

Qu'est-ce qu'un destinataire ?

Un destinataire est une personne ou un organisme qui reçoit des données personnelles pour une raison déterminée et légitime.

EXEMPLES

- L'organisateur d'un tournoi
- La fédération sportive à laquelle est rattachée un club
- Les professionnels travaillant dans la cellule de recueil des informations préoccupantes (CRIP) du département où réside l'enfant, si un membre de l'association rédige une information préoccupante afin de faire part d'une situation de danger ou de risque de danger dans laquelle se trouve un enfant

Qu'est-ce qu'un tiers autorisé ?

Un tiers autorisé est une autorité publique ou une administration autorisée par un texte (loi, décret, etc.) à recevoir les données personnelles.

EXEMPLES

- Pôle emploi ou les organismes de sécurité sociale dans le cadre de la lutte contre la fraude
- Les administrations de la justice, de la police, de la gendarmerie
- Etc

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

Un sous-traitant, qui est une catégorie de destinataires, est l'entreprise ou l'association qui manipule des données pour le compte d'un responsable de traitement dans le cadre d'un service ou d'une prestation.
Un sous-traitant a des obligations concernant les données personnelles, qui doivent être précisées dans le contrat.

EXEMPLES

- Les prestataires de services informatiques (hébergement, maintenance, etc.)
- Tout organisme offrant un service ou une prestation impliquant un traitement de données personnelles pour le compte d'un autre organisme (par exemple, la gestion de la paie des salariés de l'association etc.)

II - LES GRANDS PRINCIPES À RESPECTER

Principe de **Licéité**

Un traitement doit être licite. Pour cela, il doit :

- Poursuivre un objectif qui n'est pas contraire au droit (par exemple, un traitement de données ne peut pas avoir pour but une discrimination illégale)
- Reposer sur une base légale prévue par le RGPD

Avant de mettre en œuvre votre fichier, vous devez choisir la base légale parmi celles susceptibles d'être utilisées par une association :

- L'accord libre, spécifique, éclairé et univoque des personnes (par exemple, la prospection par voie électronique auprès de prospects, etc.)
- L'exécution du contrat (par exemple, la fourniture des prestations définies dans le cadre du contrat conclu entre l'association sportive et la personne concernée ou son représentant légal et la gestion administrative des personnes concernées)
- L'accomplissement d'une mission d'intérêt public (pour les associations de droit privé chargées d'une mission d'intérêt public ou dotées de prérogatives de puissance publique uniquement)
- La satisfaction de l'intérêt légitime de l'organisme (par exemple : la prospection par voie postale auprès des membres, etc.)
- Le respect d'une obligation légale qui impose le traitement de ces données (par exemple, lorsque l'association effectue la déclaration sociale nominative pour ses salariés)

Principe de **Finalité déterminée & légitime**

Les données doivent être collectées pour un objectif déterminé et légitime. Ce but initial poursuivi par votre organisme doit être respecté : vous ne pouvez pas utiliser les données pour une autre raison que celle qui a été fixée initialement.

EXEMPLES

Un centre musical ne peut pas transmettre les coordonnées de ses membres collectées pour l'organisation de cours à un magasin d'instruments de musique souhaitant envoyer de la publicité, si les membres n'ont pas préalablement consenti.

Principe de **Pertinence & de minimisation**

Une fois l'objectif du traitement précisément défini, vous devez déterminer les données nécessaires pour atteindre cet objectif. Ces données doivent :

- Avoir un lien direct avec l'objet poursuivi
- Être nécessaires à l'objectif poursuivi

Autrement dit, vous devez limiter autant que possible la quantité des données traitées.

EXEMPLES

Les informations relatives à la situation matrimoniale d'une personne n'apparaissent pas nécessaires dans le cadre de l'inscription à une activité sportive.

Principe de **Transparence & de respect des droits des personnes**

Les adhérents doivent comprendre pourquoi leurs données sont collectées et quels droits ils peuvent exercer. Vous devez, en conséquence, être transparent dès la collecte des données.
Les personnes concernées doivent connaître les principales caractéristiques du traitement mis en œuvre, c'est-à-dire :

- L'identité et les coordonnées de votre organisme
- L'objectif du traitement (à quoi vont servir les données collectées, par exemple, la gestion des intervenants, la gestion des adhérents, les élections au conseil d'administration, etc.)
- La base légale
- L'obligation ou non pour la personne concernée de fournir ces informations ainsi que les conséquences pour la personne en cas de non-fourniture des données
- Les destinataires ou catégories de destinataires des données (les personnes à qui sont communiquées les données. Par exemple, la fédération sportive à laquelle le club est affilié)
- La durée de conservation des données (la durée pendant laquelle les données présentent un intérêt pour votre organisme. Ensuite, les données sont supprimées ou anonymisées)
- Les droits des personnes concernées (au moins les droits d'accès, de rectification, d'effacement et à la limitation qui sont applicables pour tous les traitements)
- L'existence ou non d'un transfert de données hors de l'Union européenne (en indiquant le pays et l'outil juridique permettant de protéger les données)
- Les moyens de contacter le délégué à la protection des données de l'organisme ou du référent « protection des données personnelles »
- Le droit d'effectuer une plainte auprès de la CNIL

Ces informations doivent être présentées de manière concise et transparente. Elles doivent être adaptées à votre public (pictogrammes pour les enfants par exemple).

Pour éviter des mentions trop longues sur un formulaire, vous pouvez indiquer l'identité du responsable de traitement, l'objectif poursuivi par le traitement et les droits des personnes en fin de formulaire en renvoyant à une mention d'information complète sur le site web de l'association.

Principe de **Durée de conservation limitée**

Les données doivent être conservées pendant une durée limitée définie en fonction de l'objectif poursuivi par le traitement.
Pendant cette durée, plusieurs phases doivent être distinguées :

- Les données sont nécessaires pour la gestion courante de votre association
- Les données ne sont plus nécessaires quotidiennement mais présentent encore un intérêt administratif (par exemple, la gestion d'un éventuel contentieux) ou doivent être conservées pour répondre à une obligation légale (par exemple, les bulletins de paie des salariés de votre organisme doivent être conservés cinq ans)

Lors de la deuxième phase appelée « archivage intermédiaire », l'accès aux données doit être encore davantage limité afin qu'elles puissent uniquement être consultées de manière ponctuelle et par des personnes dont les missions le justifient (par exemple, lorsque les données passent de la « base active » à la « base d'archivage intermédiaire », elles ne doivent plus être consultables par toutes les personnes initialement prévues, mais seulement par des personnes spécialement habilitées en raison de leurs fonctions (par exemple, le service en charge du contentieux).

Une fois ces durées écoulées, vous devez :

- Supprimer les données si ces dernières ne présentent plus d'intérêt pour l'organisme
- Ou anonymiser les données à condition que les personnes concernées ne soient absolument plus identifiables

Principe de **Confidentialité & de sécurité**

Les données doivent être consultées et traitées utilisées par le moins de personnes possibles. En pratique, seuls les adhérents et salariés de l'association dont les missions le nécessitent doivent pouvoir accéder aux données traitées par votre association. Cela signifie que vous devez assurer la sécurité et la confidentialité des données afin de limiter la divulgation des données à des personnes internes ou externes qui n'ont pas besoin de les connaître.
Pour assurer la sécurité des données, vous devez prendre des mesures pour assurer la sécurité des locaux et des postes de travail.

EXEMPLES

- Fermeture à clé des locaux, armoires, bureau
- Mots de passe individuels renouvelés régulièrement, antivirus...

Les mesures de sécurité doivent être adaptées à la nature des données traitées par votre organisme et des risques qu'une divulgation pourrait représenter pour les personnes concernées (usurpation d'identité, phishing, chantage, etc.).

Lors de la suppression des données personnelles sous format « papier », vous pouvez jeter les documents dans un conteneur pour documents confidentiels ou les déchiqueter pour assurer leur confidentialité. Assurer la confidentialité des données afin de ne pas communiquer les informations à des personnes non-autorisées, vous devez vous montrer vigilant.

En interne, les habilitations informatiques doivent être gérées de sorte à ce que tout le monde ne puisse pas accéder à toutes les informations.
En cas de demande d'accès ou de communication de données par un autre organisme, vous devez vous assurer de la légitimé de la demande :

- S'il s'agit d'une autorité publique ou d'une administration autorisée par un texte à recevoir des données personnelles (par exemple, la CNIL dans le cadre de son pouvoir de contrôle) :

  - Vérifiez le texte l'autorisant à demander ces informations
  - Analysez bien la qualité de l'organisme et le périmètre des informations demandées
  - Communiquez uniquement les informations qui doivent l'être en sécurisant la transmission des données

- S'il s'agit d'une demande réalisée par un tiers ne disposant pas d'un texte autorisant cette demande :

  - Analysez la légitimité de la demande en veillant à ce que la réutilisation envisagée par l'organisme soit compatible avec la raison de la collecte des données
  - Effectuez un tri des données afin de ne communiquer que celles qui sont nécessaires à l'objectif poursuivi par l'organisme
  - Informez les personnes concernées et permettez-leur de s'opposer à cette transmission
  - Indiquez dans votre documentation ce nouveau destinataire.

En effectuant un tri des données, votre association doit analyser le niveau de détail nécessaire à l'organisme demandeur. Dans certaines circonstances, des données anonymisées ou ne permettant pas d'identifier directement la personne concernée pourront s'avérer suffisantes (par exemple, dans le cadre d'une sollicitation d'un organisme public ou privé pour l'obtention d'une subvention ou d'un mécénat, la constitution d'un dossier contenant des informations anonymisées apparaît en principe suffisant).

III - LES PREMIÈRES ÉTAPES DE LA MISE EN CONFORMITÉ

La prise en compte du RGPD ne doit pas être perçue que comme une contrainte technique ou juridique. C'est avant tout l'occasion de faire le point sur les données traitées et l'utilisation des fichiers et des services numériques dans l'association.
Le respect des règles « informatique et libertés » est une démarche continue (formation, évolution des procédures...) qui passe par plusieurs étapes.

Recenser les fichiers

Le RGPD impose de lister dans un document spécifique (le registre), les fichiers qu'il a créé ou utilise.
Ce registre permet d'avoir une vision claire et globale des activités de l'association qui nécessitent la collecte et l'utilisation de données personnelles.
Dans votre registre, créez une fiche par objectif de fichier en précisant :

- Le nom et les coordonnées du responsable du traitement et, s'ils existent, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données
- Le ou les objectifs poursuivis par chaque fichier (par exemple, la gestion des adhérents)
- Les catégories de personnes concernées et de données utilisées (par exemple, nom, adresse, etc.)
- Qui a accès aux données (c'est-à-dire les personnes habilitées comme, par exemple, le service RH pour la paie) et à qui elles seront communiquées (les destinataires, par exemple les services des impôts)
- Les durées de conservation de ces données (durée d'utilité et durée de conservation en archive)
- Les mesures de sécurité mises en œuvre (par exemple, politique de mots de passe, ...)
- Si nécessaire, les transferts de données personnelles en dehors de l'Union européenne ou à une organisation internationale

Découvrez un modèle de registre de la CNIL sur www.cnil.fr.

⚠ L'élaboration du registre nécessite d'être en contact régulier avec les adhérents, salariés et sous-traitants susceptibles de manipuler des données personnelles.

Faire le tri dans les données

Chaque fiche du registre vous permet de vérifier :

- Que les données traitées sont bien pertinentes et nécessaires à l'objectif poursuivi (principe de pertinence et de minimisation).
  Par exemple, lors de l'inscription d'un adhérent à une activité de loisirs ou à un séjour organisé par l'association, il est légitime de demander une attestation du quotient familial pour l'application d'un tarif préférentiel. Il n'est en revanche pas pertinent de demander le numéro de sécurité sociale de l'adhérent ou de son représentant légal ou encore la copie de sa carte Vitale.
- Que seules les personnes habilitées ont accès aux données dont elles ont besoin et que des mesures de sécurité adaptées sont mises en place (principe de confidentialité et de sécurité).
  Par exemple, les informations relatives au paiement des cotisations par les adhérents d'une association sportive ne doivent être rendues accessibles qu'au personnel administratif en charge de son suivi et non pas à l'ensemble des adhérents, ni même à l'ensemble des personnes en charge des entraînements.
  L'association doit définir des profils d'habilitation en séparant les droits en fonction des tâches à accomplir de chacun afin de limiter l'accès des utilisateurs aux seules données nécessaires.
- Que les données ne sont pas conservées plus longtemps que nécessaire (principe de durée limitée de conservation des données).
  Par exemple, l'association ne peut pas conserver les données concernant ses anciens membres/adhérents de manière illimitée. Elle doit les supprimer trois ans après la fin de l'adhésion de la personne.

Faire preuve de transparence

Les personnes doivent être informées à chaque fois que des données personnelles sont recueillies, sous format papier, numérique (questionnaires, bulletins d'adhésion, bulletins d'abonnement, etc.). Il est recommandé une information orale en plus d'une information écrite afin de s'assurer de la bonne compréhension par la personne concernée des informations communiquées.

Organiser & faciliter l'exercice des droits des personnes

Les personnes (adhérents, salariés, prestataires, etc.) ont des droits sur leurs données. Toute personne concernée peut ainsi :

- Obtenir la confirmation que vous traitez ou non des informations la concernant, accéder à celles-ci et en obtenir la copie
- Rectifier les informations inexactes ou incomplètes la concernant
- Faire effacer ses données (par exemple, la personne a retiré le consentement sur lequel est fondé le traitement, etc.)
- Demander la limitation ou le « gel » des données (par exemple, lorsque la personne conteste l'exactitude de ses données, celle-ci peut demander à l'organisme le gel temporaire du traitement de ses données, le temps que celui-ci procède aux vérifications nécessaires)
- Récupérer ses données pour les réutiliser (droit à la portabilité) : ce droit ne s'applique que si les trois conditions suivantes sont réunies : limitation aux seules données personnelles fournies par la personne concernée ; si les données sont traitées de manière automatisée (exclusion des fichiers par voie papier) sur la base de l'accord préalable de la personne concernée ou de l'exécution d'un contrat conclu avec la personne concernée ; respecter les droits et libertés de tiers
- S'opposer au traitement à condition d'invoquer des raisons particulières et si le traitement est mis en œuvre sur la base légale de l'intérêt légitime du responsable de traitement, ou pour l'exécution d'une mission d'intérêt public ou d'une mission relevant de l'exercice de l'autorité publique (par exemple, le responsable de traitement peut refuser à la personne concernée l'exercice de son droit d'opposition si le traitement des informations la concernant repose sur l'obligation légale)

Vous devez permettre aux personnes d'exercer facilement ces droits.

Si vous disposez d'un site web, prévoyez un formulaire de contact spécifique, un numéro de téléphone ou une adresse de messagerie dédiée. Si vous proposez un compte en ligne, donnez aux adhérents la possibilité d'exercer leurs droits à partir de leur compte. Mettez en place un processus interne permettant de garantir l'identification et le traitement des demandes dans des délais courts (un mois maximum). Si un délai supplémentaire est nécessaire pour traiter la demande (par exemple, en raison de sa complexité), la personne concernée doit en être informée dans ce même délai d'un mois. Dans tous les cas, une réponse devra être apportée dans un délai qui ne peut dépasser trois mois.

Sécuriser les données

Les incidents, internes ou externes, malveillants ou accidentels, peuvent avoir des conséquences importantes pour les personnes dont les données sont concernées (réputation, chantage, etc.).

Pour limiter les risques, vous devez mettre en place des mesures de sécurité pour empêcher :

- L'accès illégitime à des données (atteinte à la confidentialité)
- Leur modification non désirée (atteinte à l'intégrité)
- Leur disparition (atteinte à la disponibilité)

Ces risques ne sont pas théoriques. Tous les jours, la CNIL reçoit des notifications de violation de données et des plaintes dues à une sécurité insuffisante.

Les salariés et bénévoles disposent d'un identifiant propre avec un mot de passe personnel, robuste, régulièrement mis à jour et stocké de façon sécurisée au sein du système d'information. Les accès distants aux ressources de l'association, tel le back-office du site web permettant la gestion des membres, s'effectue de façon sécurisée sur un canal chiffré et authentifié (https). Leurs accès aux fichiers sont définis en fonction de leurs besoins réels en lien avec l'exercice de leur mission et leurs comptes informatiques sont clos à la fin de leur contrat. Le paiement des cotisations s'effectue sur un canal chiffré et authentifié (https). Les armoires sont fermées à clé et les accès aux locaux et serveurs ainsi que documents papiers ne sont permis qu'aux personnes en ayant nécessité.

Que faire en cas de violation des données ?

Des données personnelles ont été, de manière accidentelle ou illicite, détruites, perdues, modifiées, divulguées (courriels transmis à des mauvais destinataires, équipement perdu ou volé, publication involontaire de données sur Internet, etc.) ? Cet incident constitue une « violation de données ».
Lorsqu'un tel incident se produit, il est nécessaire de le documenter au sein de l'association. En cas de contrôle, ce document est vérifié par les services de la CNIL.
S'il existe un risque pour les droits et libertés des personnes concernées, vous devez signaler cette violation à la CNIL dans les 72 heures. Cette notification s'effectue en ligne sur le site web de la CNIL.
Enfin, si ces risques sont considérés comme élevés pour ces personnes, vous devrez les en informer. Afin de déterminer le risque pour les personnes, il convient de prendre en compte au moins les éléments suivants :

- Le type de violation (intégrité, disponibilité, confidentialité)
- La nature, le caractère sensible et le volume des données personnelles
- La facilité d'identification des personnes concernées
- La gravité des conséquences pour les personnes concernées
- Les caractéristiques particulières des personnes concernées (mineurs, personnes vulnérables, militaires, etc.)
- Les caractéristiques particulières du responsable du traitement (objet de l'association pouvant mettre en évidence des informations personnelles sensibles par exemple)
- Le nombre de personnes concernées

Une association doit-elle réaliser une analyse d'impact relative à la protection des données (AIPD) ?

Non, une association ne doit pas réaliser une AIPD sauf dans certains cas (par exemple lorsque votre fichier contient un grand nombre de données sensibles, ou bien contient des données sensibles relatives à des personnes vulnérables, ou encore dans le cas où le fichier empêche des personnes vulnérables de bénéficier d'un service).
L'analyse d'impact est un outil important pour la responsabilisation des organismes : elle les aide non seulement à construire des traitements de données respectueux de la vie privée, mais aussi à démontrer le respect des règles relatives à la protection des données.
L'AIPD se décompose en trois parties :

- Une description détaillée du traitement mis en œuvre, comprenant tant les aspects techniques qu'opérationnels
- L'évaluation juridique des caractéristiques du traitement (objectifs, données et durées de conservation, information et droits des personnes, etc.) et du respect des principes et droits fondamentaux qui sont fixés par la loi
- L'étude technique des risques sur la sécurité des données (confidentialité, intégrité et disponibilité) ainsi que leurs impacts potentiels sur la vie privée, pour déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données

IV - DES ÉLÉMENTS À UTILISER POUR ÊTRE EN CONFORMITÉ AU RGPD

Modèle de Texte

(*à compléter*) à mettre dans les formulaires de contact, pour collecter des données personnelles

Le règlement n° 2016/679, dénommé Règlement Général sur la Protection des Données (RGPD), est un règlement de l'Union Européenne qui constitue le texte de référence en matière de protection des données à caractère personnel.

Les informations personnelles recueillies dans ce formulaire sont nécessaires pour l'inscription pour le/la […]

Elles font l'objet d'un traitement informatique ou/et sur papier ayant pour finalité le/la [...]

Ces données pourront également être utilisées par les services internes à des fins de communication sur nos activités et nos actions.
Vos données personnelles sont uniquement traitées sur le territoire de l'U.E.
En application de la réglementation en vigueur, les personnes directement concernées par ce formulaire disposent d'un droit d'accès, de rectification, d'opposition, de portabilité et de suppression de leurs données à caractère personnel. Elles peuvent exercer ces droits à tout moment en adressant leur demande à l'adresse : [Mettre l'adresse mail].

Les données sont conservées conformément à la durée nécessaire aux finalités mentionnées et pour les durées de prescriptions éventuellement applicables.

Pendant toute la durée de conservation de vos données personnelles, nous mettons en place tous les moyens aptes à assurer leur confidentialité et leur sécurité de manière à empêcher leur endommagement, effacement ou accès par des tiers non autorisés.

En cas de difficulté en lien avec la gestion de vos données personnelles, vous pouvez contacter la Commission Nationale de l'Informatique et des Libertés (CNIL, plus d'informations sur www.cnil.fr) qui est l'autorité de contrôle en France pour certaines catégories de données personnelles.

Clauses RGPD entre un responsable de traitement et un sous-traitant

L'exemple de clauses de sous-traitance ci-dessous est proposé dans l'attente de l'adoption de clauses contractuelles types au sens de l'article 28.8 du règlement européen.
Ces exemples de clauses peuvent être insérés dans vos contrats. Elles doivent être adaptées et précisées selon la prestation de sous-traitance concernée. À noter qu'elles ne constituent pas, à elles seules, un contrat de sous-traitance.

[...], situé à [...] et représenté par [...]
(ci-après, « le responsable de traitement»)
d'une part,

ET

[...], situé à [...] et représenté par [...]
(ci-après, « le sous-traitant»)
d'autre part,

Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.
Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après, « le règlement général sur la protection des données »).

Description du traitement faisant l'objet de la sous-traitance

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) [...].

La nature des opérations réalisées sur les données est [...].

La ou les finalité(s) du traitement est/sont [...].

Les données à caractère personnel traitées sont [...].

Les catégories de personnes concernées sont [...].

Pour l'exécution du service objet du présent contrat, le responsable de traitement met à la disposition du sous-traitant les informations nécessaires suivantes […].

Procédure d'exercice des droits des personnes du traitement des données les concernant

Que faire en cas de demande d'accès, de rectification, de suppression, de portabilité, d'opposition ou de limitation de traitement ?

1- Si nécessaire, vérifier l'identité de la personne qui exerce une demande.
2- Si nécessaire, demandez sur quelles données porte la demande.
3- Vérifiez que la demande ne porte pas sur un tiers.
4- Répondez à la demande en respectant le délai maximum en l'espèce d'un mois pour les demandes simples et de trois mois pour les demandes complexes (par exemple, la personne demande l'ensemble du traitement de ses données).

- Si vous traitez des données concernant le demandeur, vous devrez lui fournir les informations figurant à l'article 13 ou 14 du RGPD qui figurent en principe sur tout support de collecte que vous utilisez (voir les mentions RGPD dans le texte pour le formulaire de recueil de consentement)
- Si la personne demande la copie de ses données, vous devez lui communiquer, quel que soit le support sur lequel les données sont enregistrées (document papier ou électronique, enregistrement vidéo, sonore, etc.). Le fait que des données soient contenues dans un document ne les rend pas pour autant non communicables. Il faudra, lors de la réponse, prendre en compte le droit des tiers

⚠ Vous ne pouvez pas répondre à une demande d'accès en indiquant seulement à la personne que vous disposez des données qu'elle vous avait communiquées ou en listant seulement les catégories de données dont vous disposez. Les données personnelles présentes dans un document (courrier, note, rapport, enregistrement vocal ou visuel, etc.) peuvent être communiquées par la copie du document en lui-même ou par une retranscription fidèle sur un autre support.
Les données personnelles enregistrées dans un logiciel métier peuvent être communiquées par la transmission d'impressions d'écrans ou d'une retranscription fidèle sur un autre support.

Le responsable de traitement peut-il refuser une demande d'exercice de droit ?

La réponse est OUI.

Exemple de refus au droit d'accès à des données personnelles :
Dans certains cas, vous pouvez refuser de répondre à des demandes de droit d'accès, mais vous devrez justifier cette décision.

Vous n'êtes pas tenus de répondre aux demandes de droit d'accès si :

- Elles sont manifestement infondées ou excessives, notamment par leur caractère répétitif (par exemple, demandes multiples et rapprochées dans le temps d'une copie déjà fournie)
- Les données ne sont plus conservées/ont été effacées : dans ce cas, l'accès est impossible

Sources : Règlement Général sur la Protection des Données applicable depuis le 25 mai 2018, Loi informatique, fichiers et Libertés du 6 janvier 1978 et Recommandations de la CNIL.

« ENSEMBLE, POUR UN TRAITEMENT RESPONSABLE DES DONNÉES PERSONNELLES »

Ahmadou Tidiane Ly

UNE OU PLUSIEURS QUESTIONS ?

Contactez notre Chargé de mission juridique et administratif FSGT
contact.dpo@fsgt.org - 01 49 42 23 36

Fédération Sportive et Gymnique du Travail
14 rue Scandicci - 93508 Pantin
01 49 42 23 19 - accueil@fsgt.org