GUIDE DE SENSIBILISATION AU RGPD

POUR LES ASSOCIATIONS

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr

TABLE DES MATIÈRES

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.

87 %

des Français se disent plus sensibles que ces dernières années à la protection de leurs données personnelles.[1]

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.

Pour aider les structures associatives à respecter les règles, notamment le règlement général sur la protection des données (RGPD), la CNIL propose des outils permettant de mettre en œuvre concrètement, et le plus en amont possible, les principes Informatique et Libertés.

Le respect de la réglementation en matière de protection des données personnelles est en effet nécessaire afin de créer un environnement de confiance pour les adhérents, les bénévoles, les usagers, les donateurs, les testateurs mais aussi les salariés.

Ce guide a donc pour objectif de répondre à ce besoin en aidant les associations à respecter les règles en la matière. Il comprend :

- une présentation des principales notions à connaître ;
- une présentation des grands principes à respecter ;
- un plan d'action présentant les grandes étapes de la mise en conformité ;
- une foire aux questions.

Le site web de la CNIL, qui contient déjà de nombreuses ressources pour accompagner les professionnels, sera enrichi avec des fiches issues de ce guide.

Ce guide ne répond pas à des besoins plus spécifiques et n'a pas pour objectif de présenter toutes les obligations à respecter lors de l'utilisation de données.

5 Sondage IFOP pour la CNIL réalisé auprès d'un échantillon de 1 001 personnes représentatif de la population française âgée de 18 ans et plus, décembre 2020.

INTRODUCTION

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

Le règlement général sur la protection des données (RGPD), entré en application le 25 mai 2018, reprend les grands principes déjà présents depuis 1978 dans la loi Informatique et Libertés.

Le texte abandonne la logique basée sur les déclarations à adresser à la 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 (DPO)

La désignation d'un référent ou d'un DPD / DPO, 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 à 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.

POUR ALLER PLUS LOIN

Le délégué à la protection des données (DPO) sur cnil.fr

Quelles sont les missions de la CNIL ?

La Commission nationale de l'informatique et des libertés (CNIL) est l'autorité de protection des données française. Elle poursuit quatre principales missions :

Informer et 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.

Accompagner la conformité et 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.

Anticiper et 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*.

Contrôler et 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.).

POUR ALLER PLUS LOIN

Sur cnil.fr :
• Les missions de la CNIL
• Statut et organisation de la CNIL.

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** (ex. : nom et prénom) ;
- **indirectement** (ex. : 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).

ATTENTION

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 « compagnieA@email.fr ») 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.

ATTENTION

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 ;
- ou alors 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 (ex. : 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).

POUR ALLER PLUS LOIN

Donnée sensible (définition) sur cnil.fr

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.

POUR ALLER PLUS LOIN

Le guide « tiers autorisés » sur cnil.fr

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 don- nées 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 (ex. : la gestion de la paie des salariés de l'association, etc.).

POUR ALLER PLUS LOIN

Travailler avec un sous-traitant sur cnil.fr

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 (ex. : la prospection par voie électronique auprès de prospects, etc.) ;
- **l'exécution du contrat** (ex. : 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).

POUR ALLER PLUS LOIN

Les bases légales sur cnil.fr

Principe de finalité déterminée et 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.

EXEMPLE

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.

POUR ALLER PLUS LOIN

Définir une finalité sur cnil.fr

Principe de pertinence et 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.

EXEMPLE

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

POUR ALLER PLUS LOIN

Vérifier la pertinence des données sur cnil.fr

Principe de transparence et 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** (voir « principe de licéité » p. 9) ;
- 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, voir « les grandes notions à connaître » p. 7. 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 donnée**s 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).

BONNE PRATIQUE

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.

Cet effort de transparence doit permettre aux personnes concernées d'**exercer leurs droits**. Vous devez en conséquence leur permettre de le faire aisément (voir « Organisez et facilitez l'exercice des droits des personnes », p. 15).

Principe d'une 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 :

1. Les données sont nécessaires pour la gestion courante de votre association.
2. 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 (ex. : 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 prévus, mais seulement par des personnes spécialement habilitées, ayant un intérêt à en connaître 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 .

POUR ALLER PLUS LOIN

Les durées de conservation des données sur cnil.fr

Principe de confidentialité et 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.

Assurer la sécurité des données

Pour cela, 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 ;
- Choix d'un 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.).

BONNE PRATIQUE

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.

POUR ALLER PLUS LOIN

Les conseils de la CNIL pour un bon mot de passe sur cnil.fr

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 légimité 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 t**iers 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.

BONNE PRATIQUE

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).

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.

1. Recensez les fichiers

Le RGPD impose de lister dans un document spécifique (le registre), les fichiers qu'il a créés 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 ges tion des adhérents) ;
- les catégories de personnes concernées et de données utilisées (ex. : 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 (ex. : politique de mots de passe, etc.) ;
- si nécessaire, les transferts de données personnelles en dehors de l'Union européenne ou à une organisation internationale.

ATTENTION

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

POUR ALLER PLUS LOIN

Le registre des activités de traitement (un modèle de registre de base est proposé par la CNIL) sur cnil.fr

2. Faites 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.

3. Faites 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.

POUR ALLER PLUS LOIN

Sur cnil.fr :
- Conformité RGPD : comment informer les personnes et assurer la transparence ?
- RGPD : exemples de mentions d'information

4. Organisez et facilitez 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** (ex. : 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 (ex. : 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.

BONNE PRATIQUE

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.

POUR ALLER PLUS LOIN

Respecter les droits des personnes sur cnil.fr

5. Sécurisez 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.

BONNE PRATIQUE

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.

POUR ALLER PLUS LOIN

Sur cnil.fr :
- Mots de passe : des recommandations de sécurité minimales pour les entreprises et les particuliers
- Les conseils de la CNIL pour un bon mot de passe
- Générer un mot de passe solide

Voici quelques vérifications que vous pouvez déjà effectuer :

- ☐ Les accès aux locaux sont-ils sécurisés ? (ex. : alarme, système de vidéosurveillance, etc.)
- ☐ Les armoires et coffres-forts sont-ils fermés à clés systématiquement ?
- ☐ Les comptes utilisateurs sont-ils protégés par des mots de passe d'une complexité suffisante ?
- ☐ Les comptes utilisateurs sont-ils supprimés au départ d'un utilisateur ?
- ☐ Des profils distincts sont-ils prévus selon les besoins des utilisateurs pour accéder aux données ?
- ☐ Les postes de travail sont-ils sécurisés (ex. : verrouillage automatique de session, antivirus et logiciels à jour) ?
- ☐ Les membres de l'association sont-ils sensibilisés à la protection de la vie privée ? Une charte informatique est-elle signée ?
- ☐ Des mobiles multifonctions (smartphones), ordinateurs portables ou clés USB sont-ils utilisés ? Leur usage est-il encadré ?
- ☐ Des procédures de sauvegardes régulières et de récupération des données en cas d'incident sont-elles mises en place ?
- ☐ Votre site web utilise-t-il un protocole sécurisé pour les pages sur lesquelles sont affichées ou transmises des données personnelles (ex. : authentification, formulaire en ligne) ?

POUR ALLER PLUS LOIN

Sur cnil.fr :
- Guide de sécurité des données personnelles élaboré par la CNIL
- Tous les contenus sur la cybersécurité de la CNIL

Le site www.cybermalveillance.gouv.fr vous propose également de l'aide en ligne ainsi qu'une liste de prestataires approuvés.

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.

POUR ALLER PLUS LOIN

Sur cnil.fr :
• Les violations de données personnelles
• Notifier une violation de données sur le site de la CNIL

FOIRE AUX QUESTIONS

Les communes peuvent-elles demander aux associations qu'elles subventionnent de leur transmettre le fichier de leurs adhérents ?

Non, une commune ne peut pas demander, même lorsqu'elle accorde une subvention à une association, la liste nominative de ses adhérents.

En revanche, les mairies peuvent demander la **copie certifiée du budget et des comptes de l'exercice écoulé**, ainsi que la communication de tous les documents faisant apparaître les résultats de l'activité de l'association, pour contrôler l'utilisation des subventions qu'elles ont versées.

Une association peut-elle communiquer des renseignements sur ses adhérents à des tiers autorisés ?

Oui, la communication de renseignements sur les adhérents et salariés à des « tiers autorisés » (voir p. 8) est possible à condition qu'elle repose sur un texte juridique (loi, décret, etc.).

Pour chaque demande, vous devez vous assurer que :

- **la demande de communication est écrite et repose sur un texte l'autorisant**. Vous devez vous assurer que la demande correspond bien à ce qui est permis par les textes présentés par le demandeur. Si vous avez un doute, vous pouvez interroger la CNIL (ex. : une simple demande par téléphone sans vérification particulière ne peut donner lieu à transmission de données) ;
- **le demandeur est bien cité dans le texte et est autorisé** à exiger la communication des informations ;
- **la fréquence et le périmètre de la demande de communication** (nature des données, personnes concernées et type de traitement notamment) **ne dépassent pas ce qui est prévu par la loi** (par exemple le respect du secret médical).

Vous devez veiller à ce que la transmission des informations soit réalisée de manière sécurisée (par exemple la remise en main propre, utilisation du chiffrement en cas de transmission par voie informatique, etc.).

Vous devez enfin garder des traces de la demande et de la réponse apportée en cas d'éventuel contentieux (ex. : copie de la demande, identification de l'agent ou du service demandeur, périmètre des données transmises).

POUR ALLER PLUS LOIN

Le guide « tiers autorisés » sur cnil.fr

Un membre d'une association peut-il exiger la communication de la liste de tous les autres adhérents ?

Oui, mais seulement si les statuts de l'association prévoient cette possibilité.

Une association est libre de préciser dans ses statuts que l'adhésion implique d'accepter que ses coordonnées puissent être communiquées à un adhérent qui en fait la demande, à la condition que cette communication ait un lien direct avec l'activité de l'association.

Une association sportive peut-elle publier les résultats sportifs des licenciés en ligne ?

Oui, les structures sportives peuvent publier les résultats sportifs des licenciés en ligne sous réserve du respect de certaines conditions lors de la collecte des informations :

- la personne concernée a été informée de la publication de ses résultats en ligne ;
- elle peut s'opposer à cette publication de manière simple (ex. : une case à cocher mise à sa disposition sur le formulaire de participation à une compétition sportive), en faisant valoir une situation particulière le justifiant.

Une association peut-elle publier des photos de ses membres sur son site web ou au sein de sa revue ?

Oui, sous réserve que la personne photographiée (et le responsable légal pour un mineur) aient donné leur accord à cette diffusion.

Aussi, les personnes concernées doivent autoriser la captation et l'utilisation de leur image pour des raisons précises, de préférence par écrit et vous la faire parvenir afin que vous soyez en mesure de diffuser la photographie.

ATTENTION

La publication de photographies de mineurs doit faire l'objet d'une vigilance particulière.

Une association peut-elle utiliser les données de ses adhérents pour faire des campagnes de relance des adhésions chaque année ?

Oui, une association peut utiliser les données de ses adhérents pour faire des campagnes de relance des adhésions chaque année sous certaines conditions.

La CNIL recommande que les informations relatives à un adhérent soient conservées pendant un délai de trois ans à compter de la fin de son adhésion. Pendant ce délai, et lors de chaque sollicitation, la personne concernée doit pouvoir s'opposer à l'utilisation de ses coordonnées pour des relances d'adhésion de manière simple et gratuite (ex. : un lien pour se désinscrire à la fin de chaque courriel).

Une fois le délai de trois ans écoulé, l'association devra prendre contact avec la personne concernée afin de savoir si elle souhaite continuer à recevoir de la prospection commerciale de sa part. Dans le cas contraire, ou sans réponse de sa part, la personne concernée ne devra plus recevoir de sollicitation de la part de l'association et ses données seront supprimées ou archivées.

Une association peut-elle collecter le casier judiciaire de ses salariés/bénévoles ?

Non, les associations ne peuvent pas collecter un extrait de casier judiciaire de ses salariés et/ou bénévoles.

Les organismes de droit privé ne peuvent pas traiter de données relatives aux infractions, sauf exceptions. Il s'agit d'une interdiction de principe que le consentement de la personne concernée ne lève pas.

Lors de l'adhésion à l'association, comment informer les futurs membres/adhérents du traitement de leurs données ?

Vous devez faire preuve de transparence à l'égard des personnes concernées en précisant les caractéristiques du traitement (les finalités du traitement, les durées de conservation, les destinataires, des droits dont elles disposent etc.) au moment de la collecte de leurs informations.

L'information peut être délivrée à la personne et à son représentant légal par tout moyen (ex. : des mentions d'information insérées au sein du formulaire d'adhésion à votre structure ou du livret de présentation de celle-ci, en bas des formulaires de contact, etc.) et doit être adaptée au public (ex. : des images ludiques peuvent être privilégiées lorsqu'il s'agit d'enfants, à l'oral, des pictogrammes, etc.).

Il est recommandé d'avoir recours à une information orale en plus d'une information écrite afin de s'assurer de la bonne compréhension des informations communiquées.

POUR ALLER PLUS LOIN

Sur cnil.fr :
- Les mentions d'information listées à l'article 13 du RGPD
- Conformité RGPD : comment informer les personnes et assurer la transparence ?
- Exemples de mentions d'informations.

Une association peut-elle communiquer via courrier/courriel/SMS des informations liées à l'activités de son association (évènements à venir, infolettre, etc.) à ses membre/adhérents ?

Oui, l'association peut communiquer à ses membres/adhérents via courriel/courrier/sms à condition que les personnes concernées :

- aient été **informées** de l'utilisation de leurs informations au moment de la collecte ;
- **puissent s'opposer** à recevoir ces informations.

ATTENTION

Lors de chaque envoi de courriel / SMS / courrier, la personne concernée doit être en mesure de s'opposer à recevoir les informations relatives à la vie de l'association de manière simple et gratuite (par exemple : insérer un lien de désinscription en bas de la lettre d'information ou de chaque courriel envoyé).

Une association peut-elle échanger les informations de ses adhérents à une autre association à des fins de prospection ?

Oui, une association peut échanger les informations de ses adhérents à une autre association à des fins de prospection.

Attention, les règles relatives à cette transmission diffèrent selon le type de prospection réalisée :

En matière de prospection caritative, celle-ci n'est possible que si les adhérents ont été, au moment de la collecte :

- informés de leur utilisation à des fins de prospection ;
- informés de leur possible transmission à des partenaires du secteur associatif ;
- en mesure de s'opposer, préalablement à ces utilisations, de manière simple et gratuite en cochant une case mise à leur disposition, par exemple :

☐ *Je m'oppose à ce que mes coordonnées postales ou électroniques soient utilisées pour recevoir des offres de l'association X par courrier postal ou courrier électronique.*

☐ *Je m'oppose à ce que mes coordonnées postales ou électroniques soient utilisées pour recevoir des offres des partenaires de l'association X par courrier postal ou courrier électronique.*

En matière de prospection commerciale par voie électronique, les règles applicables sont plus exigeantes : les adhérents doivent avoir explicitement donné leur accord, au moment de la collecte de leur adresse électronique, pour être démarchés par l'association ainsi que pour la transmission à un partenaire de l'association.

POUR ALLER PLUS LOIN

La prospection commerciale par courrier électronique sur cnil.fr

Une association peut-elle déposer des cookies ou des traceurs publicitaires sur son site web ?

Oui, lorsque votre site web est consulté, vous pouvez déposer des cookies et autres traceurs sur les outils utilisés par les internautes (ordinateur, tablette, smartphone, etc.) pour analyser leur navigation et leurs habitudes de consultation.

Selon l'objectif du traceur que vous utilisez sur votre site, il peut être nécessaire :

- **d'informer l'internaute de son existence** (ex. : cookie de session pour un téléservice) ;
- **d'obtenir son consentement** avant de déposer ou de lire un traceur sur son terminal.

Si votre site utilise des fonctionnalités offertes par d'autres sites (ex. : solutions de statistiques, boutons sociaux, vidéos provenant de plateformes tierces telles que Google, YouTube, Facebook, etc.), **vous devez obtenir le consentement des visiteurs.**

POUR ALLER PLUS LOIN

Sur cnil.fr :
• Site web, cookies et autres traceurs
• Comment mettre mon site web en conformité ?

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.

POUR ALLER PLUS LOIN

Sur cnil.fr :
• Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données

Commission Nationale
de l'Informatique et des Libertés
3, Place de Fontenoy - TSA 80715
75334 PARIS CEDEX 07
01 53 73 22 22

www.cnil.fr
www.educnum.fr
linc.cnil.fr

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr