Guide de sensibilisation au RGPD pour les associations

22 novembre 2021

VOTRE ASSOCIATION COLLECTE DES DONNÉES !
Et cela génère des obligation supplémentaires….

Nous sommes tous exposés à la collecte et au traitement de nos données personnelles. Nous le sommes à titre individuel en tant que citoyen attentif à notre vie privée. Et nous le sommes dans l'exercice de nos fonctions bénévoles. Car ces données sur lesquelles nous veillons jalousement, nous en collectons aussi. À chaque fois que nous demandons des informations aux bénévoles, aux adhérents… Nous constituons des fichiers qu'ils soient informatiques ou même simplement sur papier. Cela nous impose de respecter les obligations qui incombent à tout responsable de traitement qu'il s'agisse d'une personne physique ou morale, autorité publique, service ou tout autre organisme. Les associations ne font pas exception à la règle.

Un peu d'histoire :

Les années 70 marquent la naissance de l'informatique qui permet l'exploitation d'informations en nombre et décuple les capacités de fichage.
En 1974, le Ministère de l'intérieur se propose même de « croiser » les fichiers venant de plusieurs administrations, (sécurité sociale, trésor public et police…). Ce sera le déclencheur d'une inquiétude citoyenne majeure et le germe de la première réglementation protectrice du genre.

La loi n° 78-17 du 6 janvier 1978 dite « Loi Informatique et Libertés ».
Un texte précurseur qui sera modifié plusieurs fois. C'est la naissance de la CNIL (Commission Nationale de l'Informatique et des Libertés), autorité administrative indépendante auprès de laquelle il faudra déclarer ses fichiers et qui veillera à leurs protections.

La loi du 2004-801 du 6 août 2004 transposera la Directive du Parlement européen et du Conseil 95/46 du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Car l'Union Européenne veut harmoniser les législations des états membres qui ont émergé, dans le double but de protéger les données et de permettre leur libre circulation au sein de la Communauté. Avec l'énorme essor d'internet, le constat s'imposera qu'il faut « durcir » le cadre juridique.

En 2016, pas de directive cette fois, mais un règlement : Le Règlement Général sur la Protection des Données (Règlement UE 2016/679 du 27 avril 2016) ou « RGPD », entré en vigueur le 25 mai 2018.

La loi n°2018-493 du 20 juin 2018, « nouvelle » loi Informatique et Liberté qui aménage les « marges nationales » sans reprendre toutes les dispositions du RGPD.

Principales nouveautés : Il n'y a plus d'obligation de déclarer ses fichiers à la CNIL. C'est désormais aux organismes, aux associations, de se « responsabiliser » pour se mettre en conformité. L'association (donc son Président) sera pleinement responsable de la protection des données personnelles qu'elle traite.

Qu'est-ce qu'une donnée personnelle ?

Le règlement nous dit qu'il s'agit de toute information se rapportant à « une personne physique identifiée ou identifiable, directement ou indirectement ».

Attention : nous parlons bien de personnes physiques, aussi à chaque fois que vous enregistrez une personne morale (financeur, association partenaire, leur téléphone, leur mail…), vous serez en dehors du champ. En revanche, le nom et les coordonnées nominatives du représentant de la personne morale sont des données personnelles.
Par exemple les données concernant INDECOSA-CGT ne sont pas des données personnelles mais le nom de son président, son adresse mail sont des données à caractère personnelles.

Quand vous ferez remplir un bulletin d'adhésion à un consommateur, un formulaire d'inscription pour un stage à vos bénévoles, une feuille de présence pour une réunion à vos administrateurs… vous collecterez des données

personnelles : Le nom, le prénom, l'adresse, le téléphone, la profession, l'âge, une photo etc… La liste des données est longue. Quelle que soit la façon dont vous les enregistrez, vous « traitez » des données personnelles. Si vous tenez votre fichier adhérent sur papier, le RGPD s'applique. En fait la moindre intervention sur les données personnelles est un « traitement ».

Attention : seules les données personnelles utiles et nécessaires en regard du besoin (finalité de traitement) doivent être collectées. C'est le principe de minimisation qui doit être retenu.

Qu'est-ce qu'un traitement de données personnelles :

L'article 4 du RGPD indique qu'un traitement de données personnelles est « toute opération […] effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou tout autre forme de mise à disposition […] l'effacement ou la destruction.

Quels sont les droits des personnes concernées :

Le RGPD renforce la protection des personnes, elles en restent les uniques « propriétaires ». Le chapitre 3 consacre ces droits qui sont énumérés dans les articles 12 à 22. Dès la collecte, elles ont un droit à l'information, voire dans certains cas, un droit au consentement (obligatoire pour les données sensibles).

ART. 13 DROIT À L'INFORMATION

Lorsque des données à caractère personnel relatives à une personne sont collectées, le responsable du traitement doit lui fournir, au moment où les données en question sont obtenues, notamment les informations suivantes :

• l'identité et les coordonnées du responsable de traitement,
• les finalités du traitement (pourquoi ces données sont collectées, à quoi elles vont servir),
• les destinataires qui auront accès à ces données,
• les pays hors de l'Union Européenne dans lesquels pourraient être transférées ces données,
• la durée de conservation des données à caractère personnel,
• l'existence des droits des personnes (droit d'accès, de rectification et

d’effacement notamment).

ART. 14 DROIT À L’INFORMATION LORSQUE LES DONNÉES À CARACTÈRE PERSONNEL N’ONT PAS ÉTÉ COLLECTÉES AUPRÈS DE LA PERSONNE CONCERNÉE

Lorsque les données à caractère personnel n’ont pas été collectées auprès de la personne concernée, le responsable du traitement doit fournir à celle-ci les mêmes informations identifiées dans le droit à l’information (cf. art. 13).

ART. 15 DROIT D’ACCÈS

C’est le droit qui permet à toute personne physique de savoir si ses données personnelles sont traitées ou non par une entreprise. Si oui, la personne concernée a le droit d’obtenir l’accès à ses données. L’exercice de ce droit permet de contrôler l’exactitude des données et, au besoin, de les faire rectifier ou effacer (cf. art. 16). Le responsable doit être en mesure de fournir une copie des données personnelles faisant l’objet du traitement concerné. Si la demande est présentée par voieélectronique, les informations sont fournies sous une forme électronique d’usage courant, sauf demande contraire de la personne.

ART. 16 DROIT DE RECTIFICATION

Toute personne concernée peut demander la rectification des informations inexactes la concernant.
Le droit de rectification complète le droit d’accès. Il permet d’éviter qu’un organisme ne traite ou ne diffuse de fausses informations sur la personne.

ART. 17 DROIT À L’EFFACEMENT

Il étend le « droit à l’oubli ». Il permet à la personne concernée de demander l’effacement dans les meilleurs délais de ses données personnelles auprès du responsable de traitement. Ce droit peut être exercé si :

- les données ne sont plus nécessaires
- les données font l’objet d’un traitement illicite (non conforme au règlement)
- le traitement diffère de la finalité annoncée lors de la collecte
- la personne concernée retire son consentement.

Existe-t-il des limites à ce droit ? Le droit à l’effacement n’est pas absolu. Des considérations autres que les droits de l’individu peuvent primer sur l’exercice du droit à l’effacement. Ainsi, si le traitement de données personnelles relève de l’intérêt public, de la santé publique, de l’exercice de l‘autorité publique, ou encore de l’exercice de la liberté d’expression et d’information, alors le traitement

primera sur l'exercice de ce droit.

ART. 18 DROIT À LA LIMITATION DU TRAITEMENT

Toute personne a le droit d'obtenir la limitation du traitement de ses données lorsqu'elle s'y est opposée, qu'elle conteste l'exactitude des données ou que leur traitement soit illicite. De la même manière, si le responsable de traitement prévoit de détruire les données personnelles la concernant et que la personne en a besoin pour la constatation, l'exercice ou la défense de ses droits en justice, elle peut demander la limitation du traitement de destruction.

ART. 19 NOTIFICATION DE LA RECTIFICATION, DE L'EFFACEMENT OU DE LA LIMITATION DE TRAITEMENT DE DONNÉES PERSONNELLES

Afin que les droits de rectification, d'effacement ou de limitation de traitement soient respectés par tous les destinataires des données personnelles concernés, le responsable de traitement doit informer de cette demande, chaque destinataire auquel ces données ont été communiquées. Ces mêmes destinataires devront alors procéder à la rectification, effacement ou limitation tels que demandé par la personne.

ART. 20 DROIT À LA PORTABILITÉ

Lorsque le traitement est fondé sur le consentement ou sur un contrat, et effectué à l'aide de procédés automatisés, la personne concernée a le droit de recevoir ses données dans un format structuré, couramment utilisé, lisible par machine et interopérable. Elle pourra les transmettre à un autre responsable de traitement sans que le responsable du traitement initial y fasse obstacle.

ART. 21 DROIT D'OPPOSITION

C'est le droit de s'opposer au traitement de ses données personnelles, y compris le profilage, à leur diffusion, transmission ou conservation. Il peut également être exercé en cas de traitement à des fins de prospection. Ce droit est possible pour « des raisons tenant à sa situation particulière ».

ART. 22 PRISE DE DÉCISION AUTOMATISÉE

C'est le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant. Ce droit ne s'applique pas si cette décision est nécessaire à l'exécution d'un contrat ou si elle est fondée sur le consentement.

Les obligations de l’association : une collecte loyale, transparente et licite.

Vous avez une obligation d’information (art.13 du RGPD), vous devrez fournir : les coordonnées de votre association, les catégories de données que vous collectez (nom, prénom, courriel…), l’origine de la collecte.
La base légale du traitement (consentement, contrat, obligation légale, sauvegarde des intérêts vitaux, intérêts publics ou intérêts légitimes, le caractère obligatoire ou non du traitement, les destinataires (votre association régionale, nationale, des partenaires), le responsable du traitement (l’association représentée par son président) et surtout la question principale de la finalité (pour quoi faire ?).

Votre obligation à la clarté, la lisibilité, vous impose d’être concis. Pas question de noyer le lecteur dans un document si long qu’il ne le lira pas. Aussi vous fournissez les informations essentielles et vous renverrez le consommateurs, l’adhérent, le bénévole à un document plus exhaustif précisant tous les droits. Vous pouvez le remettre lors des permanences en document papier par exemple, en ligne si vous avez un site internet.

Dans le cas d’un site internet, vous devez mettre en visibilité les mentions d’information : les conditions générales d’utilisation, la politique de protection des données personnelles, la gestion des cookies, les modalités d’exercice des droits accessibles aisément. Vous pouvez faire une affiche. Il faut juste pouvoir prouver que cette information a été mise à disposition.

Pour renseigner vos documents : formulaire d’adhésion, bulletin d’inscription aux formations, abonnement à votre revue associative. La CNIL vous propose des modèles.

En principe, il est interdit de gérer certaines données personnelles dites « sensibles ». Les données sensibles concernent l’origine ethnique ou raciale, les opinions politiques, les convictions religieuses ou philosophiques ou l’appartenance syndicale, les orientations sexuelles, la santé.
Vous pourrez enregistrez l’appartenance syndicale car pour vous, elle est légitime. Mais pour les autres, en principe, c’est non. Cependant, dans l’animation de vos permanences juridiques, vous en collecterez. Pas à grande échelle, c’est vrai… mais vous en collecterez.

Exemples :
• *Il s'agit d'un différend d'assurance invalidité ? vous aurez des informations sur la santé de votre adhérent, des certificats médicaux dans votre dossier, noté l'information dans votre fichier.*
• *Vous défendez une locataire victime de violences conjugales, pour mettre fin à la solidarité concernant le bail ? Vous aurez collecté des données « sensibles » : certificat médical mais aussi ordonnance du juge aux affaires familiales (le relevé d'infraction est en principe interdit).*

Pour la gestion des litiges, vous demanderez un consentement préalable, en insérant une case particulière, à cocher. Vous disposerez ainsi de la preuve (à garder précieusement) que vous avez obtenu le consentement de votre adhérent, expressément. Le consentement doit être fait en 2 exemplaires (un pour la personne et un pour INDECOSA) et doit être conservé par INDECOSA aussi longtemps que la durée indiquée sur le consentement lui-même (c'est-à-dire aussi longtemps que les données personnelles collectées). À échéance de la durée de conservation, les données personnelles doivent être détruites de façon irréversible ainsi que le consentement lui-même.

Ce consentement doit de plus comporter des informations très précises quant au traitement des données personnelles dans ce cadre.
Le consentement doit être :

– spécifique : il doit expressément mentionner à quoi vont servir les données personnelles (finalités de traitement). Il faut s'assurer que le consentement est adéquat et précise le type de données collectées.

– éclairé : avant de signer, la personne doit recevoir toutes les informations nécessaires pour décider de donner son consentement.
En plus d'être explicite et précis, pour qu'un consentement soit valide, il doit être accompagné des informations suivantes :

– L'identité du responsable de traitement : INDECOSA votre association régionale, nationale, des partenaires
– Les finalités de traitement : dans quel(s) but(s) INDECOSA utilise les données personnelles
– Les catégories de données collectées : données d'identification, photos, données sensibles (de santé, ethniques…) ;

– L'existence des droits que peuvent exercer les personnes (retrait, modification, suppression…)
– Les destinataires des données personnelles
– La durée de conservation des données personnelles (Par exemple 2 ans à compter de la fin du litige)
– à la fin du consentement une case sera à cocher par la personne avec la mention, » *Je consens à ce que l'association INDECOSA-CGT de : ……. , traite mes données sensibles dans le cadre de la gestion du litige que je lui confie* ».

Quelles procédures mettre en place au sein de l'association ?

Ce qu'on attend de vous, c'est que vous dominiez l'ensemble de vos fichiers, il n'est pas question qu'ils soient éparpillés, difficiles à retrouver Un recensement s'impose en se demandant à quels moments et pour quelles activités, vous collecterez des données. La « finalité », vous l'avez vu, fait partie des informations obligatoires à donner.

Exemple de « finalités » : *pour suivre les cotisations des adhérents, pour organiser des formations pour vos équipes, pour constituer des dossiers pour les litiges de vos adhérents (qu'ils soient stockés sur ordinateur ou dans une pochette*).

Faites le point, en équipe, de toutes vos activités. C'est le moment de mobiliser les compétences internes.
Renseignez un registre, qui en fera la liste (en format papier ou numérique). Il permettra de « centraliser » les informations, précisera la durée de conservation des données personnelles par finalité de traitement et la façon dont vous archivez. La durée de conservation des données pour une même finalité de traitement doit être la même au niveau national ou régional. Ainsi les données collectées pour les formations ne seront identiques au niveau national et au niveau régional. Ce registre s'avérera utile pour vous organiser au mieux. Si vous le renseignez bien, en l'actualisation régulièrement, il sera plus simple de vérifier que vous respectez bien les règles fixées par le RGPD.

Faites du tri. Toutes les données collectées, enregistrées au fil du temps, vous sont-elles vraiment nécessaires ? Car vous devez respecter le principe de minimisation qu'impose le RGPD. La durée de conservation est un autre élément

important qui doit être obligatoirement porté à la connaissance de la personne intéressée mais le RGPD ne donne pas de consigne précise de « temps ». Vous allez les définir en fonction des activités.

Les données personnelles vont avoir un « cycle de vie » au sein de votre association. Elles commenceront par figurer dans votre « base active », vos adhésions en cours, etc… Ce sera le cas également pour les litiges, tant que le dossier est en cours. À ce stade, les données seront accessibles aux personnes en charge de leur traitement … Et puis un jour, les dossiers seront clos.
À partir de là, ils passeront en « statut inactif » », sous le contrôle d'un nombre restreint de personnes (à désigner) … mais sans devoir y rester indéfiniment… C'est à ce stade, qu'il vous faut déterminer des « temps ».

Pour certaines activités, vous pourrez vous contenter de 3 années à partir du dernier contact. Mais vous pouvez souhaiter conserver les données personnelles de vos bénévoles plus longtemps, pour des projets futurs, des projets festifs ou des évènements à venir. Ce sera possible mais vous devez prévoir cette durée, l'expliquer (pourquoi ?) et la consigner. La justification des durées de conservation est l'une des informations que la CNIL vérifie en premier lors d'un contrôle.

Les obligations légales de conserver des données seront votre repère, quand il y en a. Si vous avez un salarié dans l'association, par exemple, la loi vous impose de conserver ses bulletins de salaire durant 5 années, impossible de prévoir moins (L3243-4 du Code du travail) mais certaines données qui intéressent sa retraite future doivent être conservées jusqu'au bout. Dans le cas d'un salarié la quasi-totalité des données personnelles qui sont collectées le sont sur les bases légales du traitement que sont le contrat (de travail) et l'obligation légale de l'employeur (par exemple de connaître le n° de sécurité sociale de son salarié). Dans ce cas les durées de conservation sont celles indiquées dans le code du travail, le CGI…

Pour les dossiers juridiques, vous pouvez tenir compte des temps de prescription. Que conserver et combien de temps pour se protéger d'un éventuel contentieux ? Car vous exercez une mission de conseil (dans le cadre d'une obligation de moyen), votre responsabilité pourrait être recherchée. Pour mémoire, la prescription civile de droit commun est de 5 ans. Donc vous définissez un « temps » par catégories de données où vous donnez les éléments d'appréciation que vous avez retenu. Et vous penserez à contrôler ce temps qui passe… pour ne pas

conserver dans vos registres (informatique ou papier.) des données au-delà. Il faudra faire du tri régulièrement, purger.

Autre obligation majeure de votre association : la sécurité. Veillez à la protection des données en interne. Tous les bénévoles de l'association ne doivent pas y avoir accès. Aussi, désignez des responsables. Vous êtes tenus à la confidentialité, au respect de l'intégrité des données (pas de modifications, d'altérations) et à la disponibilité aux personnes autorisées.

Sécuriser les données passera par des mesures physiques : fermeture du bureau, rangement du classeur ou des dossiers dans une armoire qui ferme à clé… Si vous partagez vos locaux avec d'autres associations, par exemple, vous veillerez à ce que vos fichiers ne soient pas accessibles.
Il ne suffit pas qu'un bureau « puisse » être fermé à clé, il doit l'être ! Il n'est pas obligatoire d'isoler les informations quand elles sont au stade d'archives mais c'est conseillé. Faites des sauvegardes.

Vous prendrez des mesures informatiques, en veillant à la mise à jour des antivirus et de vos logiciels, en changeant régulièrement le mot de passe… En cas de vol du matériel informatique ou de piratage (nous ne sommes pas à l'abri de phishing.) et ce sera plus sûr.

Mais des failles de sécurité peuvent provenir d'un problème technique, d'un accident, d'une mauvaise manipulation voire de l'intervention d'un tiers mal intentionné (phishing). Vous documenterez la nature de la violation, les données et le nombre de personnes concernées, les
conséquences possibles et les mesures de correction prises.

En cas de faille de sécurité, pouvant constituer un risque pour les droits et libertés des adhérents, des salariés, des partenaires…

Si la violation n'entraîne pas de risque pour les droits et libertés des personnes concernées, INDECOSA devra documenter, en interne, sous forme de registre, la violation qui s'est produite. Il ne sera pas utile de notifier cette violation ni à la CNIL ni aux personnes concernées. Il faut en revanche absolument documenter cet incident car sa documentation pourra être contrôlée par la CNIL.

Si la violation entraîne un risque pour les droits et libertés des personnes concernées, INDECOSA devra documenter sous forme d'un registre la violation

qui s'est produite, notifier cet incident à la CNIL dans un délai maximal de 72 heures.

Si la violation entraîne un risque élevé pour les droits et libertés des personnes concernées, INDECOSA devra documenter sous forme d'un registre la violation qui s'est produite, communiquer en priorité la violation aux personnes concernées et notifier cet incident à la CNIL dans un délai maximal de 72 heures.

Vous faut -il un délégué à la protection des données (DPD) ou data protection officer (DPO) ?

Le DPD a pour rôle de conseiller et de veiller au bon respect du RGPD par le responsable du traitement (donc ça ne peut pas être la même personne !). Il est obligatoire d'en désigner un pour les acteurs qui gèrent un nombre massif de données et pour la gestion de données sensibles, (ex : ethnie, santé…) à grande échelle.

Vous ne gérez pas de données à si grande échelle sur vos territoires, donc vous n'êtes pas dans cette obligation. Mais vous pouvez le faire, vous pouvez désigner une personne de l'association qui sera responsable, mais ce ne pourra pas être la personne qui traite les données, car on ne peut pas être juge et partie. Ou vous pouvez mutualiser un DPD avec d'autres associations. Vous définirez également qui peut accéder à quelles données.

Que faire en cas de demande d'une personne dont vous avez collecté les données ?

Le RGPD dispose que lorsqu'une personne exerce ses droits (ex. réception d'une demande de droit d'accès ou de suppression), l'association doit lui répondre « sans tarder » et au maximum dans un délai d'un mois à compter de la réception de la demande. L'envoi des documents, pour l'exercice du droit d'accès, est en principe gratuit.

Si vous ne pouvez pas répondre, vous devrez obligatoirement indiquer les motifs du refus ainsi qu'indiquer la possibilité d'introduire une réclamation auprès de la CNIL et de former un recours juridictionnel.

Le rôle de la CNIL

La CNIL (Commission Nationale Informatique et Libertés) est l'autorité

administrative indépendante qui vieille sur nos données personnelles, notre vie privée. Elle dispose d'un site sur lequel vous trouverez une mine d'informations, des conseils de méthode et de nombreux outils (guides, modèles de mention, des modèles de registres, des téléservices).

Elle a bien sûr une mission de contrôle, a posteriori, des organismes qui traitent nos données. Elle pourrait donc être amenée à vous contrôler. Il convient de lui répondre immédiatement en cas de demande. Elle peut vous interroger à distance, faire un contrôle sur pièces ou même venir sur place. Vous serez réactifs.

Le RGPD a renforcé les possibilités de sanctions de la CNIL. Elle dispose d'une gamme de moyens, elle peut faire des rappels à l'ordre, des mises en demeures sous astreinte, elle aussi prononcer des sanctions financières importantes. Selon les manquements, la sanction peut aller jusqu'à 10 millions d'€ ou 2 % du chiffre d'affaires mondial, ou jusqu'à 20 millions ou 4 % du chiffre d'affaires mondial.

Deux exemples de sanctions prononcées en 2020 par la CNIL (consultables sur le site) :
Un médecin qui n'avait pas suffisamment protégé ses ordinateurs, sa connexion : 6000 €.
Un magasin de la grande distribution qui envoyait des sollicitations commerciales sans
consentement des destinataires : 2.225. 0000€.

INFO Pratique N°7*| 25 mars 2021 |RGPD | collecte des données / obligations générées.* indecosa@cgt.fr – *indecosa.fr*