COMMENT GÉRER LES LISTES DE CONTACTS ET LES LISTES D'ENVOIS ?

Doit-on avoir un consentement positif « opt-in » pour tous nos envois de newsletter ou appels aux dons ?

◢ **Pour les listes de contact** que vous aviez avant l'entrée en vigueur de la RGPD : vous n'êtes pas obligé de demander un renouvellement du consentement positif mais vous devez vous assurer que les destinataires aient la possibilité de se désinscrire ou de contacter sans difficulté votre organisation pour effacer leurs données si elles le désirent.

◢ **Pour toutes les données collectées après le 25 mai 2018,** il est demandé un consentement positif à l'exception des courriers postaux toutes boites.

◢ Il est obligatoire de recueillir une autorisation explicite et transparente **pour vos envois vers vos donateurs ou membres**. Ce consentement doit être obtenu pour chaque type de traitement et l'utilisation finale des données récoltées, l'abonné doit avoir le choix. **Par exemple :** Un consentement est nécessaire pour l'envoi d'une newsletter, un second pour l'envoi de matériel pour une campagne de récolte de fonds, un troisième pour les invitations à des évènements.

Qu'entend-t-on par consentement positif ?

Le RGPD défini le consentement positif de la manière suivante. « Le consentement doit être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale »

Ce consentement doit pouvoir être retiré aussi simplement qu'il a été donné.

Il faut donc idéalement pour chaque contact :

- mettre en place un mécanisme de recueil du consentement « opt-in » et de rétractation « opt-out » ;
- préciser les principales caractéristiques du traitement (objet, finalité, durée, etc.) afin que la personne sache clairement à quoi elle consent ;
- démontrer avoir obtenu le consentement de la personne ;
- consigner et conserver la charge de la preuve du consentement dans le registre des activités de traitement (date, heure, etc.) ou en l'absence de ce dernier, tout autre support aisément consultable par l'autorité de contrôle me dispensant du consentement exprès.

COMMENT GÉRER LES DROITS À L'IMAGE ?

Le RGPD considère qu'une photographie d'une personne est une donnée à caractère personnel.

En règle générale avant de prendre une photo ou une vidéo d'une personne, vous devez lui demander son autorisation mais cela ne veut pas dire qu'elle consent à la publication ou à la diffusion de ces images. Il y a donc deux consentements distincts à prendre en compte de l'utilisation de son image.

La question du droit à l'image qui comprend le droit de publication et de prise de vue sont complexes. De nombreux facteurs interviennent pour analyser la légalité de la publication d'une photo sans consentement explicite.

Afin d'être certain de ne pas enfreindre les lois et règlements, il est préférable de prendre les mesures suivantes :

- Avertir les participants que vous allez prendre des photos pendant un événement et que vous allez éventuellement utiliser les photos.

- Recueillir le consentement des participants pour la prise de photo et la publication ultérieure. Pour ce faire vous pouvez une liste de présence avec une case à cocher qui autorise la publication de photos pour pouvoir prouver le consentement par la suite.

- Pour les photographies en milieu scolaire ou les photographies de mineurs, il faut le consentement des représentants légaux. Il faut donc prévoir un formulaire type qui sera signé par les représentants légaux. En milieu scolaire, il faut analyser avec l'établissement scolaire qu'elles sont les accords signés en relation avec le droit à l'image avec les représentants légaux lors d'activités organisées par des organisations tierces.

- Si vous n'avez pas de consentement explicite pour la publication ou si vous avez des doutes, il est préférable de flouter les visages des personnes qui peuvent être reconnues sur la photo.

Qu'en est-il des photos provenant des projets ?

En principe, d'un point de vue éthique, il faut appliquer les mêmes mesures avec la prise de photographie lors des visites sur le terrain. D'un point de vue légal, il convient également de se référer aux lois nationales en vigueur.

Afin de vous éclairer sur ce sujet vous pouvez vous référer aux documents publiés :

Le Règlement Général sur la Protection des Données : Le droit à l'image. (CNPD, 2018)

Fiche pratique relative à l'utilisation de photos ou vidéos en milieu scolaire. (CNPD, 2018)

Le guide illustré : Code de conduite en matière de message et images. (Dochas & Cercle de Coopération, 2017)

COMMENT GÉRER LES DONNÉES PERSONNELLES LIÉES À L'ADMINISTRATION DE L'ORGANISATION ET LA GESTION DU PERSONNEL ?

Pour la gestion quotidienne de l'organisation beaucoup de données sont collectées et traitées. Il peut s'agir de la gestion des cotisations des membres, de la gestion du personnel, des données concernant des fournisseurs ou des données personnelles enregistrées dans les logiciels de gestion financière. Les 6 principes de la RGPD s'appliquent également ici.

Les données liées au personnel

Concrètement, il faut tacher de traiter avec précaution les données liées au personnel surtout les données qui peuvent être sensibles comme les certificats pour les absences, les commentaires et évaluations.

La durée de garde des données relatives à un employé doit être limitée dans le temps. Les données doivent être détruites après le départ d'un employé. Certaines données peuvent être gardées jusque 3 ans pour des raisons administratives ou de gestion et certaines jusque 10 ans quand elles sont indispensables pour un audit financier ultérieur. Ici également le principe de minimisation ou d'anonymisation des données prévaut.

Au sein de l'organisation les données relatives au personnel doivent être sécurisées et les autorisations d'accès limitées au maximum. Les employés doivent pouvoir avoir accès à l'information les concernant.

Si des personnes vous envoient des CV lors de procédures d'embauche, il faut demander leur autorisation pour les garder. Sans autorisation préalable, il faut supprimer les CV de votre base de données.

Les données personnelles en relation avec le travail sur le terrain (données des bénéficiaires ou partenaires) tombent-elle sous le coup de la RGPD ?

Toute donnée qui est traitée sur le sol européen est soumise à la RGPD. Les ONG sont donc responsables de traiter de la même manière les données provenant des pays partenaires et les données collectée au Luxembourg.

Dans la mesure du possible, déléguez la gestion de ces informations à votre partenaire. Si vous avez besoin de cette information pour des rapports ou des comptes rendus vers les donateurs et les bailleurs de fonds, tachez de minimiser les données et de les anonymiser quand cela est possible.

Il est important également de sensibiliser votre partenaire sur la gestion des données personnelles et de vous assurer que les lois en vigueur dans leur pays soient respectées.

COMMENT S'ASSURER QUE LES SOUS-TRAITANTS RESPECTENT LE RGPD ?

Les ONG confient des fichiers contenant des données personnelles à des fournisseurs pour la prestation de certains services. Ce peut être une liste d'adresse pour un imprimeur qui envoie les documents, des fichiers envoyés à un auditeur, l'hébergeur de votre site internet, vos service de cloud ou des services de partage de fichiers. Il est de votre responsabilité de vous assurer que ces données seront gardées et traitées en conformité avec le RGPD pour cela les mesures suivantes sont à considérer :

- Choisir des sous-traitants de confiance
- Choisir des sous-traitants basés en Europe ou qui s'engagent à se soumettre au RGPD européen
- Faire signer une contrat avec le sous-traitant

Le RGPD impose que les relations entre responsable de traitement et sous-traitant de données soient strictement encadrées et formalisées dans un contrat écrit. Ce contrat doit contenir un certain nombre de mentions et de clauses obligatoires parmi lesquelles on compte une clause autorisant le responsable de traitement à auditer la manière avec laquelle le sous-traitant traite les données pour son compte ou encore une clause organisant l'accès du personnel du sous-traitant aux données.

Voici le lien vers un contrat-type

COMMENT ASSURER LA SÉCURITÉ DES DONNÉES PERSONNELLES ?

La sécurité des données personnelles se réfère principalement à la manière dont sont sécurisés vos bases de données au sein de votre réseau informatique et vos ordinateurs.

Pour plus d'information vous pouvez vous rérérer au document de la CNIL, France. Ce document contient une procédure en 17 étapes pour améliorer la sécurité informatique dans votre organisation.

La checklist «Sécurité informatique» se base sur ce document.

QUE FAIRE EN CAS DE VIOLATION DE DONNÉES ?

Si vous pensez que votre site ou votre base de données a été piratée ou si vous avez perdu un ordinateur, vous devez notifier à la CNPD dans les 72 heures qui suivent le moment du constat. Si l'attaque ou la perte est susceptible d'entrainer un risque pour les droits et les libertés des personnes présentes dans la base de données vous devez également les avertir.

Pour en savoir plus sur la violation des donnés

Accès aux formulaires de notification de violation de données de la CNPD