Le Règlement Général sur la Protection des Données

Un guide pratique pour le monde associatif

Contenu

Préface

Le règlement général sur la protection des données[1] (ci-après : « le RGPD ») s'applique depuis le 25 mai 2018 dans tous les Etats membres de l'Union européenne. Dès que vous collectez et traitez des données à caractère personnel et que vous êtes établis sur le territoire de l'Union, vous êtes bel et bien soumis au RGPD, indépendamment de votre taille, de votre forme juridique, de vos activités ou de votre objet social.

Le RGPD prévoit donc le nouveau cadre légal au niveau européen à respecter en matière de protection des données. Au Grand-duché, il remplace la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Le système des formalités préalables (notifications et autorisations) auprès de la Commission nationale pour la protection des données (ci-après : « la CNPD ») prévu par ladite loi modifiée du 2 août 2002 n'existe plus. Tous les acteurs établis sur le territoire luxembourgeois doivent être en mesure de démontrer eux-mêmes leur conformité.

Ce guide vise à donner un aperçu et une guidance générale en matière de protection des données aux associations sans but lucratif (ci-après de manière générale: « les associations » ou « vous »). Il s'adresse principalement et surtout aux associations dont l'activité se limite à effectuer des traitements de données habituels et nécessaires à la gestion d'une association dite « classique » ou « traditionnelle ». Il n'est pas adapté à guider de manière exhaustive des associations qui de par la nature de leurs activités traitent des données personnelles (en termes de volume, de sensibilité, etc.) pour des finalités qui dépassent ce cadre habituel (p.ex les associations sans but lucratif visées par la loi « ASFT »[2] qui œuvrent dans le domaine social, familial, thérapeutique, etc.).

[1] Le règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
[2] La loi modifiée du 8 septembre 1998 réglant les relations entre l'Etat et les organismes œuvrant dans les domaines social, familial et thérapeutique.

Rappel de quelques notions élémentaires

- Le responsable du traitement est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement, qui décide donc « pourquoi » et « comment » des données personnelles sont collectées et traitées.

Pour une association, ses différents services, ses groupements locaux, ses dirigeants, ainsi que ses collaborateurs, pour autant qu'ils soient actifs dans le cadre de l'exécution des tâches de l'association, constituent un seul responsable du traitement. Par contre, ses membres, tout comme ses organes faîtiers sont en principe à considérer comme tiers par rapport à l'association.

- Le sous-traitant est la personne physique ou morale qui traite des données personnelles pour le compte et sur instruction du responsable du traitement dans le cadre d'un service ou d'une prestation.

- Une donnée à caractère personnel est toute information se rapportant à une personne physique identifiée ou identifiable. Une personne peut être identifiée :
- directement (p. ex. par son nom, prénom, ou une adresse mail nominative) ;
- indirectement (p. ex. par un identifiant (n° membre), un numéro (de téléphone), une donnée biométrique (ses empreintes digitales), plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image).

L'identification d'une personne physique peut être réalisée :
- à partir d'une seule donnée (p. ex. le nom et prénom ou une adresse mail personnelle) ;
- à partir du croisement d'un ensemble de données, même sans indiquer le prénom et le nom de la personne concernée (exemple : un sportif, né à telle date qui lors d'une compétition spécifique ayant lieu tel et tel jour, qui a atteint un record national pour la discipline des 100 mètres).

Si on est en présence de données anonymes ou anonymisées (des informations rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable, ni par le responsable du traitement, ni par un tiers), le RGPD ne s'applique pas. Or, comme l'illustre l'exemple ci-dessus du sportif ayant atteint un record national, de temps à autre la simple suppression du nom, prénom et adresse ne suffit pas pour anonymiser tout un set de différentes données. Dans ce cas, on parle de données pseudonymisées qui tombent dans le champ d'application du RGPD.

- Un traitement de données personnelles est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé. Le RGPD nomme toute une série de différents types de traitement comme la collecte, l'enregistrement, la modification, la diffusion ou toute autre forme de mise à disposition, ou encore l'effacement et la destruction.

Un traitement de données personnelles n'est pas nécessairement informatisé : les dossiers papier (pour autant qu'ils soient structurés comme p.ex par un classement alphabétique / chronologique) sont également concernés et doivent être protégés dans les mêmes conditions.

En plus, le RGPD ne s'applique pas aux données à caractère personnel des personnes décédées, comme par exemple lors de la publication d'une notice nécrologique d'un ancien membre dans le journal d'une association, mais sous condition de respecter la dignité et la vie privée des proches du défunt.

Pour résumer voici un exemple illustrant les différentes notions : Un club de sport, représenté par son Président et les autres membres du comité (organe décisionnel), est à considérer dans son ensemble comme responsable du traitement en définissant pourquoi et comment des données sont collectées et traitées. Le club décide notamment de créer un tableau Excel, contenant la liste de ses membres actifs et non-actifs. Cette liste comprend les informations suivantes : noms, prénoms, adresses postales et adresses mail. Ce fichier sert à envoyer des newsletters et comme moyen de convocation aux assemblées générales. Le club de sport a engagé une société WWW pour lui créer un site internet via lequel les personnes peuvent adhérer ou recevoir des informations.

Les données recueillies sont des données à caractère personnel, car elles permettent d'identifier clairement les membres. Les données sont recueillies pour des finalités précises : la gestion administrative des membres, l'envoi de newsletters et la convocation aux assemblées générales. Les différentes opérations comme la collecte et l'envoi des informations sont des traitements distincts. Finalement, la société WWW est à considérer comme sous-traitant du club de sport en agissant uniquement pour le compte et sur instruction de ce dernier.

➔ **Voir l'article 4 du RGPD concernant les définitions des différentes notions.**

L'établissement du registre

Parmi les obligations incombant au responsable du traitement, figure en premier lieu l'établissement d'un registre des activités de traitement. La première étape consiste donc à inventorier et à recenser de façon précise vos différents traitements de données personnelles. L'élaboration d'un registre des traitements vous permet ainsi de faire le point. Toutes les associations devront en principe établir un tel registre pour les traitements de données qui ont un caractère répétitif (tel que par exemple : la mise à jour de la liste des membres, la gestion des cotisations, l'actualisation du site internet, si applicable l'enregistrement à des compétitions, etc.). Il n'est pas obligatoire de préciser les traitements de données occasionnels dans le registre.

Identifiez donc vos activités qui nécessitent la collecte et le traitement de données personnelles et créez pour chaque activité recensée une fiche spécifique en fonction de la finalité poursuivie. Les données sont généralement collectées par des associations pour les finalités suivantes : gestion administrative des membres, gestion du site internet, envoi de newsletters, gestion des fournisseurs, gestion des cotisations, gestion de la comptabilité et la gestion des listes de contact (« VIP ») autres que les membres pour l'envoi d'invitations à des événements. En fonction d'autres activités spécifiques supplémentaires d'une association, des données peuvent être collectées pour d'autres finalités comme par exemple la gestion des salariés, la lutte contre le dopage ou encore la gestion du contrôle médico-sportif.

Chaque fiche doit préciser principalement (c'est-à-dire une fiche par traitement de données et par finalité):

- l'objectif poursuivi (la finalité – voir les exemples ci-dessus) ;
- les catégories de personnes concernées (exemple : tous les licenciés) ;
- les catégories de données utilisées (exemple pour les licenciés : nom, prénom, adresse postale, adresse mail et date de naissance ; attention : le registre doit contenir uniquement les catégories de données et en aucun lieu les données personnelles en elles-mêmes) ;
- les destinataires des données (une fiduciaire, un ministère, l'organisateur d'un tournoi, etc.) ;
- la durée de conservation de ces données (ne doit pas être plus longue que nécessaire pour atteindre les finalités prévues, à analyser au cas par cas) ;
- le cas échéant, les transferts de données vers un pays tiers ou à une organisation internationale.

Un modèle d'un registre avec des exemples concrets se trouve en annexe, qui doit être adapté au cas par cas en fonction de l'activité et des finalités des traitements de données de l'association.

➔ **Voir l'article 30 du RGPD concernant le registre des activités de traitement.**

La légitimité du traitement de données à caractère personnel

Chaque traitement de données doit respecter et être basé uniquement sur un des six critères de légitimité prévus par le RGPD : le consentement, l'exécution d'un contrat, une obligation légale, la sauvegarde des intérêts vitaux, une mission d'intérêt public ou encore l'intérêt légitime.

➔ **Voir l'article 6 du RGPD concernant la licéité du traitement.**

Dans des cas marginaux, des textes légaux peuvent prescrire des traitements de données par une association qui ont une incidence sur ses activités (le Code du travail, la loi modifiée du 21 avril 1928 sur les associations et les fondations sans but lucratif, les dispositions en matière de sécurité sociale et d'impôts, dans le cadre de la lutte anti-dopage, etc.). Par exemple, le Code Antidopage de l'Agence Luxembourgeoise Antidopage, qui transcrit les règles et principes énoncés au Code Mondial Antidopage, oblige ladite Agence à rapporter publiquement l'issue d'une procédure antidopage, en précisant, entre-autres, le nom du sportif ou de l'autre personne ayant commis la violation.

Or, de manière générale, trois critères de légitimité peuvent entrer en ligne de compte dans le cadre du traitement de données par une association:

1. Le recueil du consentement

Attention : La personne doit avoir un choix réel de refuser le traitement et elle doit au préalable avoir reçu les informations mentionnées ci-dessous. Par ailleurs, par la mise en place de différentes cases à cocher, une personne doit avoir la possibilité d'accepter un traitement (p.ex : recevoir la newsletter) tout en refusant un autre (p.ex. l'utilisation des données à des fins de marketing). Les cases cochées par défaut sont interdites.

Voici quelques exemples pratiques, où le recueil du consentement apparaît nécessaire et approprié:

- publication de données de contact privées des membres d'un comité sur votre site internet ;
- publication dans une revue d'information des dates de naissance des nouveau-nés des membres, ainsi que leurs dates de mariage ;
- inscription à une newsletter ;
- transfert des données de contact des licenciés d'un club sportif à un magasin de sport ;
- transfert des données de contact des personnes inscrites dans des séances d'un groupe d'entraide à une autre association ;
- publication des noms des sponsors externes (personnes physiques) à une association, ainsi que le montant des dons ;
- mise en place d'un groupe « What'sApp » par un entraîneur pour communiquer avec les joueurs et leurs parents et sous condition de leur proposer une alternative en cas de refus.

Attention : Pour les mineurs, le consentement des représentants légaux est requis. Lorsqu'un enfant a atteint l'âge de discernement ou « l'âge de raison », qui se situe selon la jurisprudence actuelle entre 12 et 14 ans, le double consentement du parent et de l'enfant est recommandé, afin de tenir compte de la volonté de l'enfant.

Le consentement ne doit pas nécessairement se manifester par un formulaire écrit, mais peut aussi ressortir de tout autre déclaration ou acte positif clair, par laquelle une personne accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Par exemple, par le fait de payer les cotisations pour sa carte de membre, une personne accepte de figurer sur la liste des membres d'une association et de recevoir chaque année une demande de renouvellement de son abonnement. Néanmoins, pour des moyens de preuve (envers vos membres et lors de contrôles réalisés par la CNPD), il est recommandé de documenter de quelle manière le consentement a été recueilli. Or, il ne saurait y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité.

2. Si le traitement de données s'avère nécessaire à l'exécution d'un contrat auquel la personne concernée est partie. Par exemple, pour exécuter le contrat de travail d'un salarié d'une association, le recueil de diverses données est nécessaire (en principe le nom, prénom, adresse, date de naissance, numéro d'identification national et le compte bancaire). Dans ce cas, le recueil du consentement n'est pas le fondement approprié pour le traitement de données.

   Encore, l'appartenance à une association peut dans certains cas et en fonction des statuts et des activités poursuivies (prestations de services offertes) être considérée comme relation contractuelle entre les membres et l'association elle-même. Or, les traitements des données concernant les différents membres ne doivent pas dépasser ce qui est nécessaire pour exécuter ledit contrat (en principe limité au nom, prénom, adresse, année de naissance et le compte bancaire).

3. Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par l'association, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel. Voici quelques exemples :
   - Publication sur son site internet d'une liste des noms, prénoms et années de naissance des joueurs d'un club sportif ;
   - Envoi aux héritiers d'une personne décédée d'une liste des donateurs et des montants des dons reçus ;
   - Publication sur le site internet des noms, prénoms et adresses mail professionnelles des membres du comité ;
   - Publication temporaire des noms, prénoms et années de naissance des joueurs sélectionnés pour un match et les résultats des compétitions ;
   - Transmission des données des joueurs et membres à l'organisateur d'un tournoi ;
   - Transmission de données des joueurs à une fédération en vue d'obtenir une licence.

Attention aux intérêts et droits fondamentaux des personnes concernées, ainsi qu'au principe de minimisation des données. Collectez et traitez uniquement les données nécessaires pour atteindre les objectifs prévus. Par exemple : A moins de disposer du consentement, l'indication sur un site web d'un club sportif de la date de naissance exacte et de la nationalité des joueurs, ainsi que des adresses privées des membres du comité dépasserait le strict nécessaire et constituerait une ingérence dans la vie privée des personnes concernées.

Attention : Une association n'est pas en droit de traiter les données pour une autre finalité que celle pour laquelle elle les a collectées. Par exemple, une association ne peut transmettre les données de ses membres à un magasin de vêtements afin que ce dernier leur envoie de la publicité, sauf à avoir le consentement préalable des membres.

Cas particulier des données dites « sensibles »

Une vigilance particulière est nécessaire en cas de traitement de données sensibles (p.ex. l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, les données de santé ou des données concernant la vie sexuelle ou l'orientation sexuelle). Par principe, il est interdit de traiter de telles données, sauf si une des dix conditions prévues au RGPD est remplie, comme par exemple :

- le consentement explicite des personnes concernées ;
- une obligation en matière de droit du travail ;
- le traitement est effectué par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, à condition que ledit traitement se rapporte exclusivement aux membres et que les données ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées ;
- les données sont manifestement rendues publiques ;
- …

➔ **Voir l'article 9 du RGPD concernant le traitement de données dites « sensibles ».**

Attention au droit à l'image

Le droit à l'image signifie que toute personne a sur son image et l'utilisation qui en est faite un droit exclusif et peut s'opposer à une diffusion non autorisée par elle. Alors même qu'il n'existe pas de texte spécifique portant sur le droit à l'image en droit luxembourgeois, la jurisprudence en la matière l'a clairement consacré. En effet, la plupart de ces décisions judiciaires se fondent sur l'article 1 de la loi du 11 août 1982 concernant la protection de la vie privée, qui dispose que « *chacun a droit au respect de sa vie privée* ».

En principe, chaque personne concernée doit donner son consentement préalable pour la prise, ainsi que pour la publication de sa photo. Pour la prise et la publication de photos de mineurs, le consentement des représentants légaux est requis, et à partir de l'âge de discernement, également le consentement du mineur. Si une association est amenée à prendre et publier des photos de mineurs au cours de ses activités, la CNPD recommande de soumettre une fois par an un formulaire de consentement auxdits représentants et le cas échéant aux mineurs en précisant clairement pour quelles finalités des photos peuvent être prises et sur quels supports les photos peuvent être publiées (internet, intranet, journal d'une association, sur les réseaux sociaux, etc.), tout en leur permettant d'accepter la publication sur un support et non sur un autre.

Dans les autres cas, le consentement à la prise de vue peut aussi se manifester par un acte positif clair, comme par exemple le fait de poser lors d'une fête de fin d'année d'une association pour une photo prise par une personne appartenant à l'association. Encore, si un membre d'une association participe à une réunion d'information sur un sujet spécifique et s'il est indiqué sur la porte d'entrée que des photos seront prises pour illustrer la réunion sur le site internet de

l'association, ce membre donne son consentement en entrant dans la salle de réunion. Néanmoins, une personne peut retirer son consentement en demandant au photographe de supprimer ses photos sur son appareil et/ou de les retirer d'un éventuel site en cas de publication.

Comme quasiment chaque droit, le droit à l'image connaît aussi des exceptions, comme en cas de prévalence du droit à la liberté d'expression qui comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations (comme par exemple l'illustration d'une activité d'une association sur son site internet ou la publication d'un article de presse sur un événement d'une association). Lors d'une manifestation publique organisée par une association, des photos peuvent donc être prises et publiées sur différents supports, sans consentement des personnes concernées. Si un individu s'oppose à cette publication, l'association doit, dans la mesure du possible, respecter cette opposition et, à titre d'illustration, retirer l'image (la photo individuelle) ou flouter la personne concernée.

Dans tous les cas, le droit des personnes concernées d'être informées, tel qu'expliqué ci-dessous, est à respecter.

Vous pouvez consulter dans ce contexte sur notre site internet notre guidance spécifique et plus détaillée relative au droit à l'image.

L’information des personnes concernées

En vertu du principe de la transparence, vous devez informer de manière appropriée toutes les personnes desquelles vous collectez et traitez des données (membres, licenciés, clients, fournisseurs, etc.), indépendamment du critère de légitimité tel qu’expliqué précédemment.

Vérifiez que l’information comporte notamment les éléments suivants :

- votre identité et vos coordonnées ;
- pourquoi vous collectez les données (« la finalité » ; p. ex. pour gérer la liste de vos membres) ;
- ce qui vous autorise à traiter ces données (le « fondement juridique » : un des six critères de légitimité mentionnés ci-dessus) ;
- qui sont les destinataires des données (p. ex. une fédération, le service du contrôle médico-sportif, l’organisateur d’un tournoi, etc.) ;
- si vous transférez des données hors de l’Union européenne (précisez le pays et assurez-vous que des garanties appropriées encadrent ces transferts, p.ex. lorsque vous utilisez une plateforme cloud hébergée aux Etats-Unis d’Amérique) ;
- combien de temps vous conservez les données (p. ex. : aussi longtemps qu’une personne est membre d’une association) ;
- les droits des personnes concernées tel qu’expliqué ci-dessous ;
- le droit d'introduire une réclamation auprès de la CNPD.

Pour éviter des mentions trop longues au niveau d’un formulaire papier ou en ligne, vous pouvez par exemple donner un premier niveau d’information en fin de formulaire et renvoyer à votre politique de confidentialité ou à une page dédiée à la vie privée sur votre site internet qui doit inclure toutes les mentions ci-dessus. À l’issue de cette étape, vous avez répondu à votre obligation de transparence.

➔ **Voir les articles 12 à 14 du RGPD concernant l’information des personnes concernées.**

Le respect des droits des personnes concernées

Les personnes dont vous traitez les données ont des droits sur leurs données, qui sont d'ailleurs renforcés par le RGPD. Il s'agit essentiellement des droits suivants :

- le droit à l'information: voir ce qui est décrit ci-dessus ;
- le droit d'accès: le droit d'obtenir l'accès à ses données et d'en recevoir une copie ;
- le droit de rectification: le droit d'obtenir la rectification des données inexactes ;
- le droit à l'effacement (ce qu'on appelle encore le droit à l'oubli): le droit d'obtenir du responsable du traitement l'effacement des données pour différents motifs (p. ex. si une personne retire son consentement sur lequel est fondé le traitement). Néanmoins, il ne s'agit pas d'un droit absolu. Par exemple, si la conservation des données est nécessaire pour respecter une obligation légale, le droit à l'oubli n'est pas applicable ;
- le droit d'opposition: le droit de demander qu'il soit mis un terme au traitement de ses données personnelles pour des raisons tenant à sa situation particulière, sauf si le responsable démontre l'existence de motifs légitimes et impérieux prévalant ou si le traitement est prévu par la loi.

En ce qui concerne l'envoi de publicité, une distinction s'impose selon le mode utilisé. En cas d'envoi de publicité par courrier postal, le RGPD confère aux personnes concernées un droit de s'opposer (« opt-out ») à tout moment, mais leur consentement préalable n'est pas nécessaire. Ainsi, une association peut envoyer des flyers d'informations via courrier postal ou des demandes de dons à ses propres membres, si elle permet aux personnes contactées de s'y opposer (par exemple en leur fournissant un coupon-réponse ou une adresse mail spécifique permettant d'exprimer leur souhait de ne plus recevoir de tels courriers).

En cas d'envoi de publicité par courriel électronique, la loi luxembourgeoise modifiée du 30 mai 2005[3] continue à s'appliquer aux communications électroniques. Deux situations distinctes peuvent se présenter dans ce cas :

1. si une association a obtenu des coordonnées électroniques dans le cadre d'une relation préexistante (p. ex. lors de la vente d'une carte de membre), elle peut les utiliser à des fins publicitaires sans consentement préalable. En contrepartie, les personnes concernées doivent avoir le droit de s'y opposer à tout moment (et être informé de ce droit lorsque les données sont recueillies, ainsi que lors de chaque message de prospection).

2. si aucun lien entre une association et un individu n'existe, le consentement préalable doit être demandé avant l'envoi de courriels électroniques (« opt-in »).

Une association doit donner aux différentes personnes concernées les moyens d'exercer effectivement leurs 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 à vos membres 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 (1 mois au maximum).

[3] La loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

Veillez à ne pas garder les données plus longtemps que nécessaire. Si par exemple un membre d'une association démissionne, ces données sont en principe à supprimer.

Si un individu a l'impression que vous ne respectez pas ses droits, il peut contacter la CNPD.

- ➔ **Voir les articles 13 à 21 du RGPD concernant les droits des personnes concernées.**

Le délégué à la protection des données

Le délégué à la protection des données occupe une place importante au sein du cadre juridique créé par le RGPD. Il a une mission d'information, de conseil et de contrôle du respect des règles prévues en matière de protection des données. Le DPO fait en plus office de point de contact pour la CNPD.

En principe, le traitement de données personnelles n'est pas au cœur de l'activité quotidienne d'une association, mais il s'agit d'une activité accessoire, indispensable pour son fonctionnement, sa gestion et son administration. La nomination obligatoire d'un DPO est donc très rare dans ce domaine.

Il est obligatoire de désigner un DPO si une des trois conditions suivantes s'applique :

1. vous êtes une autorité publique ou un organisme public (pas applicable) ;
2. vos activités de base consistent en des opérations de traitement exigeant un suivi régulier et systématique à grande échelle des personnes concernées (en principe pas applicable) ;
3. vos activités de base consistent en un traitement à grande échelle de données sensibles ou relatives à des condamnations pénales et à des infractions (rarement applicable).

Il s'avère dès lors que parmi ces trois cas de figures, uniquement le dernier est susceptible de s'appliquer aux associations, comme par exemple dans le cadre d'un réseau national d'aides et de soins à domicile traitant des données de santé à grande échelle. Certaines associations peuvent aussi nommer un DPO en commun, qui peut être soit un membre du personnel (DPO interne), soit exercer ses missions sur base d'un contrat de service (DPO externe).

Ses coordonnées sont à communiquer au public (une adresse mail spécifique sur le site internet sera suffisante) et à la CNPD par le formulaire de nomination accessible sur son site.

➔ **Voir les articles 37 à 39 du RGPD concernant le DPO.**

La sous-traitance

Vous pouvez en votre qualité de responsable du traitement confier la gestion de certains traitements de données personnelles à des prestataires externes (p. ex. pour la mise en place, ainsi que la gestion technique de votre site internet, pour l'enregistrement des données sur les serveurs mis à dispositions par un tiers, pour l'utilisation d'un cloud, la gestion administrative de vos membres, un comptable qui calcule les salaires, etc.).

Vous ne pouvez faire appel qu'à des sous-traitants qui présentent des garanties suffisantes quant au respect de la règlementation en matière de protection des données (vous devez le vérifier et en avoir la preuve).

En cas de sous-traitance, l'établissement d'un contrat de sous-traitance est nécessaire. Ce contrat doit lier les deux parties, prévoyant, entre-autres, que le sous-traitant ne peut traiter les données à caractère personnel pour ses propres fins, mais uniquement sur instruction du responsable du traitement. Des clauses types relatives aux règles du RGPD doivent s'y retrouver.

Le RGPD renforce les obligations imposées au sous-traitant. Par exemple, il doit aussi établir un registre des activités de traitement, il doit notifier au responsable du traitement toute violation de données à caractère personnel, et il peut aussi être soumis à l'obligation de nommer un DPO.

➔ **Voir l'article 28 du RGPD concernant le sous-traitant.**

D’autres obligations plus spécifiques

Une analyse d’impact relative à la protection des données (articles 35 et 36 du RGPD) est requise au préalable en cas de traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Les associations ne seront que très rarement confrontées à une telle obligation.

Une violation des données personnelles (articles 33 et 34 du RGPD) ne peut jamais être exclue à cent pour cent (des attaques par des hackers, perte de la liste des membres, perte d’un ordinateur portable ou d’un stick USB). Cette violation est tout d’abord à enregistrer dans votre registre interne (ce registre est obligatoire et indépendant de votre registre de traitement). Ensuite, vous avez en principe l’obligation de notifier la violation à la CNPD dans les 72 heures et dans certains cas, aussi aux personnes concernées. Un formulaire de notification d’une violation de données se trouve sur le site de la CNPD.

Des règles spécifiques sont prévues pour d’éventuels transferts de données vers des pays tiers (hors Union européenne) ou à une organisation internationale (articles 44 à 49 du RGPD) et les personnes concernées par ces transferts doivent en être informées au préalable. Tel est par exemple le cas si vous choisissez pour l’envoi de vos newsletters un prestataire de services qui offre ses services en Europe, mais qui transfère les données dans des pays en dehors de l’Union européenne (p.ex. les Etats-Unis d’Amérique, la Chine, l’Inde, etc.). De manière générale, la CNPD vous recommande de vérifier dès le départ si des prestataires établis dans l’Union européenne vous offrent les mêmes services, car ces derniers sont soumis aux mêmes règles en matière de de protection des données.

Vous êtes obligés de mettre en place des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (article 32 du RGPD). Les principes de la protection des données dès la conception et par défaut (article 25 du RGPD) sont très importants. Ils impliquent que, par défaut, uniquement les personnes au sein d’une association qui ont besoin pour l’exécution de tâches particulières aient accès aux données personnelles en cause. Par exemple, le comité d’une association doit pouvoir accéder aux données des membres afin d’assumer toutes ses tâches. Par contre, le trésorier d’une association ne doit pas avoir accès à l’ensemble des données des différents traitements de données, mais, le cas échéant, uniquement à celles qui sont nécessaires pour pouvoir assumer ses tâches comme par exemple la gestion des cotisations, la tenue des livres comptables et pour effectuer des virements bancaires.

Vous pouvez par ailleurs consulter nos deux brochures *(« Vos obligations en matière de protection des données »* et *« Vos données? Vos droits! »*), ainsi que notre page dédiée au RGPD sur notre site internet.

Annexe 1 : Modèle d'une notice d'information

Attention : Ce document constitue uniquement un modèle d'une notice d'information, qui reprend les informations obligatoires prévues par l'article 13 du RGPD. Les points 1 à 4 doivent être complétés et adaptés au cas par cas en fonction des activités et des finalités des traitements de données de l'association en cause. Ladite notice est à publier au minimum sur le site internet de l'association, sinon et en plus dans les documents et correspondances destinés aux personnes concernées.

1. Nom et données de contact du responsable du traitement

Nom de l'association, adresse postale, numéro de téléphone, adresse mail, site internet et éventuellement les noms des membres du comité.

2. Finalités, base de légitimité du traitement et catégories de données traitées

L'association traite les données suivantes :

- Pour la gestion administrative des membres (sur base du consentement / d'un contrat) : nom, prénom, adresse postale, adresse mail, date d'adhésion ;
- Pour l'envoi de newsletter (sur base du consentement): nom, prénom, adresse postale, adresse mail ;
- Pour la gestion des fournisseurs (sur base d'un contrat) : nom et prénom de la personne de contact, adresse postale, adresse mail, numéro de téléphone ;
- Pour la gestion des cotisations (sur base du consentement / d'un contrat) : nom, prénom, adresse postale, adresse mail, compte bancaire ;
- Pour la gestion des listes de contact autres que les membres : nom, prénom, adresse postale, adresse mail ;
- Pour la gestion des salariés[4] (sur base d'un contrat): nom, prénom, CV, adresse postale, adresse mail, numéro d'identification national, date de naissance, classe d'impôt, casier judiciaire, compte bancaire, salaire, certificats de maladie ;
- Pour la gestion des licenciés (sur base du consentement / d'un contrat) : nom, prénom, adresse postale, adresse mail, date de naissance, photo ;
- …
- **(à adapter au cas par cas)**

3. Catégories de destinataires des données traitées

- Dans le cadre de la gestion administrative des membres, des données sont transférées aux membres exerçant une fonction interne (le Comité, le secrétaire, le trésorier, etc.) ;
- Pour l'envoi de newsletter, des données sont transférées à un prestataire de service externe ;
- Les données des salariés sont transférées à une fiduciaire pour l'établissement des fiches de salaire ;
- Les données des licenciés peuvent être transmises à l'organisateur d'un tournoi et au contrôle médico-sportif ;
- Toutes les données sont stockées par une entreprise sous-traitante située au Luxembourg ;
- …
- **(à adapter au cas par cas)**

[4] Si applicable: les salaries doivent être informés individuellement.

4. Durée de conservation

- Données des membres : 1 année après :
  - le non-paiement de la cotisation annuelle
  - qu'un membre quitte l'association
  - l'exclusion d'un membre
  - …
  - **(à adapter au cas par cas)**

- Données traitées dans le cadre de la gestion des cotisations : 2 mois après clôture annuelle des comptes ;
- …
- **(à adapter au cas par cas)**

5. Droits des personnes concernées

Vous pouvez accéder aux données vous concernant et en obtenir une copie (article 15 du RGPD), obtenir la rectification de données inexactes ou incomplètes (article 16 du RGPD), vous opposer au traitement de vos données dans les conditions prévues par l'article 21 du RGPD et obtenir l'effacement de celles-ci dans les conditions prévues par l'article 17 du RGPD. Vous disposez dans certains cas d'un droit à la portabilité (article 20 du RGPD) et à la limitation du traitement dans les conditions prévues par l'article 18 du RGPD.

6. Réclamation

Si vous estimez que le traitement de vos données effectué par nous constitue une violation du RGPD, vous pouvez introduire une réclamation auprès de la CNPD (www.cnpd.lu).

Annexe 2 : Illustration d'un registre des activités de traitement sur base de l'article 30 du règlement général sur la protection des données

Attention : Ce document constitue uniquement un modèle d'un registre des activités de traitement, qui reprend une liste exemplative et non exhaustive des traitements habituels d'une association. Les différentes rubriques doivent donc être complétées et adaptées au cas par cas en fonction des activités et des finalités des traitements de données de l'association.

Nom et coordonnées du responsable du traitement : Nom de l'association, noms des membres du comité, adresse postale, numéro de téléphone, adresse mail, site internet, dernière mise à jour[5]

	Finalité	Catégories de personnes concernées	Catégories de données traitées	Catégories de destinataires	Transferts vers des pays tiers	Délais prévus pour l'effacement des données	Mesures de sécurité organisationnelles et techniques
Traitement n°1	Gestion administrative des membres	Membres de l'association	• Nom, • Prénom • Adresse postale • Adresse mail • Date d'adhésion • etc.[6]	• Imprimerie des cartes de membres • Service cloud • Membres exerçant une fonction interne (le secrétaire, etc.) • etc.	N.A.[7]	1 année après : • non-paiement de la cotisation annuelle • avoir quitté l'association • l'exclusion d'un membre • etc.	• Contrôle d'accès du fichier • Mesures de traçabilité • Mesure de protection des logiciels • etc.
Traitement n°2	Gestion des cotisations	Membres	En plus du traitement n°1 : compte bancaire	Membres exerçant une fonction interne (le trésorier, etc.)	N.A.	2 mois après clôture annuelle des comptes	Idem

[5] L'association doit vérifier régulièrement (+/- 1 fois par an) que le registre est à jour.
[6] A chaque fois que le présent document mentionne « etc. », l'association doit adapter et compléter le contenu de la rubrique en cause à sa situation concrète.
[7] En principe non applicable.

Traitement n°3	Newsletter	Tous ceux y ayant consenti	• Nom • Prénom • Adresse postale • Adresse mail • etc.	Prestataire de services externe	N.A.[8]	Jusqu'au retrait du consentement	Idem
Traitement n°4	Gestion du site internet	• Membres • Visiteurs du site	• Adresse I.P. • Cookies • etc.	Prestataire de services externe	N.A.	A déterminer au cas par cas	Idem
Traitement n°5	Publication de photos sur le site internet	• Membres • Spectateurs • Autre tiers	Photos prises lors d'évènements	Visiteurs du site	N.A.	Jusqu'au retrait du consentement	Idem
Traitement n°6	Gestion des listes de contact (« VIP ») non membres	• Politiciens • Commerçants • Sponsors • etc.	• Nom, • Prénom • Adresse postale • Adresse mail • etc.	N.A.	N.A.	Jusqu'à opposition de la personne concernée	Idem
Traitement n°7	Gestion des fournisseurs	Fournisseurs	• Nom et prénom de la personne de contact • Adresse postale • Adresse mail • Numéro de téléphone • etc.	• Fiduciaire • Membres exerçant une fonction interne (le trésorier, etc.) • etc.	N.A.	• 10 ans	Idem
Traitement n°8	Gestion des salariés	Salariés	En plus du traitement n°1 : • CV • Numéro d'identification national • Classe d'impôt • Casier judiciaire • Date de naissance	• Fiduciaire • Membres exerçant une fonction interne (le Comité, etc.) • Impôts • Sécurité sociale • etc.	N.A.	• 3 ans après résiliation du contrat de travail • casier judiciaire : 1 mois à partir de la conclusion du contrat de travail • etc.	Idem

[8] A faire attention si ledit prestataire de services, offrant ses services en Europe, transfère les données dans des pays en dehors de l'Union européenne.

			• Compte bancaire • Salaire • Certificats de maladie • etc.				
Traitement n°9	Vidéo-surveillance pour la protection des biens (locaux, installations, équipements, etc.)	Membres et autres usagers des locaux	Images	• Membres exerçant une fonction interne (le Comité, etc.) • Sous-traitant (une société de gardiennage) • Police • Autorités judiciaires • etc.	N.A.	8 jours	Idem
…							

COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

1, avenue du Rock'n'roll I L-4361 Esch-sur-Alzette
Tél. : (+352) 26 10 60 - 1 I Fax. : (+352) 26 10 60 - 29

www.cnpd.lu