CONSIGNES RGPD

Que sont les données personnelles ?
Selon la CNIL (Commission nationale de l'informatique et des libertés), il s'agit de l'ensemble des données relatives à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement par un numéro d'identification ou des éléments qui lui sont propres (nom, adresse IP, adresse postale...).

La SNEMM est-elle concernée ?
Depuis le 25 mai 2018, le Règlement Général sur la Protection des Données (R.G.P.D.) doit être appliqué par toutes les organisations publiques ou privées.
L'association est donc concernée et doit, pour être conforme au R.G.P.D., être garante de toutes les données à caractère personnel qu'elle collecte, leur usage et d'en protéger l'accès aux personnes non autorisées.

Rappel des grands principes du RGPD.

La SNEMM doit obtenir le consentement des personnes physiques pour lesquelles elle recueille dans le cadre de ses acticités des données personnelles :
La SNEMM doit être en mesure de démontrer que les données personnelles collectées sont dûment autorisées par la partie concernée.

La gestion du consentement implique que la personne concernée puisse donner son accord à ce que l'association collecte des données personnelles dans le cadre de son activité, et puisse le retirer.

Cet accord peut se faire notamment en cochant une case sur le bulletin d'adhésion ou d'inscription ou au moyen d'une autre déclaration ou d'un autre comportement indiquant clairement dans ce contexte que la personne concernée accepte le traitement proposé de ses données à caractère personnel. Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité.

La mise en place du RGPD nécessite d'être en mesure d'assurer cinq grands principes pour protéger les données personnelles :

- ➔ le principe de finalité : on ne peut conserver et utiliser les données personnelles d'une personne physique que dans un but précis, légal et légitime. Pour une association, son but non lucratif est un but précis et légitime mais il ne peut conserver, ni recenser d'autres informations qui ne seraient pas utiles pour ce but.

- ➔ le principe de proportionnalité et de pertinence : les données personnelles conservées doivent être strictement nécessaires au regard de la finalité voulue. L'association ne peut détenir plus de données que celles nécessaires à la réalisation des prestations.

- ➔ le principe de durée de conservation limitée : on ne peut pas conserver une donnée personnelle de manière indéfinie, sa durée de conservation doit être fixée à l'avance puis supprimée au-delà de ce temps prévu.

- ➔ le principe de sécurité et de confidentialité : les données que l'on détient ne doivent pas pouvoir être accessibles à autrui et seules les personnes autorisées doivent y avoir accès. L'association doit être garante des données qu'elle possède et en assume la responsabilité en cas de fuites en informant la CNIL.

- ➔ le principe de reconnaissance du droit des personnes : ce principe comprend le droit d'information, le droit d'accès, le consentement. Une personne est en droit de refuser de transmettre ses données, mais elle risquerait de ne pas pouvoir bénéficier des prestations et services proposés par l'association.

Le registre des activités de traitement : centre névralgique du dispositif RGPD.

Qu'est-ce que le registre des activités de traitement ?

L'obligation de tenir un registre des traitements concerne tous les organismes, publics comme privés et quelle que soit leur taille, dès lors qu'ils traitent des données personnelles.

A quels objectifs doit répondre ce registre ?

Ce registre permet de recenser sous forme de fiches la manière dont sont traitées les données personnelles et de disposer d'une vue d'ensemble de ce qui en est fait. Le registre est prévu par l'article 30 du RGPD. Il participe à la documentation de la conformité.

C'est un document d'analyse, il doit refléter la réalité des traitements de données personnelles et permet d'identifier précisément :

- ✓ les parties prenantes (représentant, sous-traitants, co-responsables, etc.) qui interviennent dans le traitement des données ;
- ✓ les catégories de données traitées ;
- ✓ à quoi servent ces données (ce qui en est fait), qui accède aux données et à qui elles sont communiquées :
- ✓ combien de temps elles sont conservées ;
- ✓ comment elles sont sécurisées.

Au-delà de l'obligation légale de rédaction, quels sont les avantages pour la SNEMM de mettre en place et d'utiliser un tel registre ?

Au-delà de la réponse à l'obligation prévue par l'article 30 du RGPD, le registre est **un outil de pilotage et de démonstration** de notre conformité au RGPD. Il permet de documenter les traitements de données et de poser les bonnes questions :

- ✓ ai-je vraiment besoin de cette donnée dans le cadre de mon traitement ?
- ✓ Est-il pertinent de conserver toutes les données aussi longtemps ?
- ✓ Les données sont-elles suffisamment protégées ? Etc...

Sa création et sa mise à jour sont ainsi **l'occasion d'identifier et de hiérarchiser les risques au regard du RGPD. Cette étape essentielle permet d'en déduire un plan d'action de mise en conformité** des traitements aux règles de protection des données.

A quel niveau la SNEMM est-elle tenue de mettre « le curseur » ?

Les entreprises et entités de moins de 250 salariés telle que la SNEMM bénéficient d'une dérogation en ce qui concerne la tenue de registres.

Ils doivent seulement inscrire au registre les seuls traitements de données suivants :

- ✓ les traitements non occasionnels (exemple : gestion de la paie, gestion des clients/prospects et des fournisseurs, etc.) ;
- ✓ les traitements susceptibles de comporter un risque pour les droits et libertés des personnes (exemple : systèmes de géolocalisation, de vidéosurveillance, etc.) ;
- ✓ les traitements qui portent sur des données sensibles (exemple : données de santé, infractions, etc.).

Quelles fiches de traitement ont été rédigées dans le cadre du RGPD/SNEMM ?

Une fiche de registre doit être établie pour chacune des activités principales de la SNEMM (grâce à la dérogation il n'est pas nécessaire de rédiger une fiche concernant les traitements non occasionnels).

Ainsi, à la suite de l'audit réalisé et des consignes du RGPD un registre de traitement a été rédigé. Celui-ci intègre les cinq fiches suivantes :

- ✓ fiche « Gestion des Adhérents et des membres bienfaiteurs » ;
- ✓ fiche « Chancellerie » ;
- ✓ fiche « Gouvernance de la SNEMM » ;
- ✓ fiche « Gestion des ressources humaines de l'association » ;
- ✓ fiche « Gestion de la résidence autonome ».

Que doit consigner une fiche de traitement ?

Pour chaque activité de traitement, la fiche de registre doit comporter au moins les éléments suivants :

- ✓ le nom et les coordonnées du responsable du traitement mis en œuvre ;
- ✓ les finalités du traitement (l'objectif en vue duquel la SNEMM a collecté ses données) ;
- ✓ les catégories de personnes concernées (adhérents, bénévoles, salariés, etc.) ;
- ✓ les catégories de données personnelles (exemples : identité, situation familiale, économique ou financière, données bancaires, données de connexion, donnés de localisation, etc.) ;
- ✓ les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées/accessibles, y compris les sous-traitants auxquels vous recourez ;
- ✓ les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale et, dans certains cas très particuliers, les garanties prévues pour ces transferts ;
- ✓ les délais prévus pour l'effacement des différentes catégories de données, c'est-à-dire la durée de conservation, ou à défaut les critères permettant de la déterminer ;
- ✓ une description générale, des mesures de sécurité techniques et organisationnelles misent en œuvre pour protéger les données.

La durée de conservation des données personnelles : quand purger ?

La durée de conservation des données personnelles. Ce cycle connaît trois phases :

1) **Conservation en base active.** Il s'agit de la durée nécessaire à la réalisation de l'objectif (finalité du traitement) ayant justifié la collecte/enregistrement des données.

2) **Archivage intermédiaire.** Les données personnelles ne sont plus utilisées pour atteindre l'objectif fixé (« dossiers clos ») mais présentent encore un intérêt administratif pour l'organisme (ex : gestion d'un éventuel contentieux, etc.) ou doivent être conservées pour répondre à une obligation légale (par exemple, les données de facturation doivent être conservées dix ans en application du Code de commerce, même si la personne concernée n'est plus adhérente). Les données peuvent alors être consultées de manière ponctuelle et motivée par des personnes spécifiquement habilitées ;

3) **leur destruction.**

En cas de non-respect du principe de conservation limitée des données, l'article 83.5 du RGPD prévoit une amende administrative pouvant s'élever jusqu'à 20 M€ (dans le cas d'une entreprise, jusqu'à 4% du chiffre d'affaires annuel).

La durée de conservation des données personnelles.

Dans le cadre de la rédaction du registre des traitement, nous avons dû pour chaque catégorie de données définir une durée de conservation (durée au-delà de laquelle les données doivent être supprimées).

- ❖ Ainsi, concernant les données relatives **aux adhérents et membres bienfaiteurs** de l'association, il a été défini la durée de conservation suivante :

  « Ainsi, les données relatives à la gestion des adhérents et des membres bienfaiteurs sont conservées en base active tant qu'ils continuent à cotiser. Les données passent ensuite en archivage intermédiaire (armoire et système d'information) **durant 10 ans**. Cette durée se justifie par le fait qu'il arrive régulièrement qu'une réadhésion ait lieu plusieurs années après la fin d'une période de cotisation. Au-delà de ce terme, l'association procède ensuite à la destruction des données personnelles des adhérents ».

- ❖ Concernant les données relatives aux résidents, il a été défini la durée de conservation suivante :

  « Les données relatives au suivi des résidents sont conservées en base active pour chaque résident tant que celui-ci est hébergé au sein de la résidence. Sont conservées dans ce cadre toutes les données personnelles nécessaires à un hébergement digne. Les données passent ensuite en archivage intermédiaire (armoire et système d'information) **pendant 10 ans**. Cette durée se justifie par les formalités nécessaires et les éventuels litiges. Les données relatives aux résidents sont ensuite détruites ».

- ❖ Concernant les données relatives aux membres chargés de la gouvernance de la SNEMM, il a été défini la durée de conservation suivante :

  « Concernant les membres chargés de la gouvernance de l'association et ses salariés, leurs données personnelles sont conservées par l'association tant que les besoins administratifs susceptibles de

recourir à ces données sont nécessaires. Les données en lien avec la gestion de la paye des salariés de l'association sont conservées 5 ans ».

En parallèle des purges ici évoquées, il est recommandé de ne pas conserver dans les messageries de l'association des mails (boite d'envoi, de réception mais aussi de suppression) de façon illimitée. Les messageries sont en-effet « truffées » de données personnelles.

➔ ainsi, compte tenu des différents délais du purge évoqués, il parait plus pratique de n'en retenir qu'un seul pour la purge des messageries. Cette méthode est d'autant plus facile que cela évite de devoir trier spécifiquement les mails.

➔ dans ce cadre, il faut supprimer les mails des messageries de l'association qui ont plus de 5 ans.

La sécurisation des données détenues par la SNEMM.

- Si le risque zéro n'existe pas, il faut prendre les mesures nécessaires pour garantir au mieux la sécurité des données. C'est une obligation légale d'assurer la sécurité des données personnelles détenues.
- L'importance des mesures à prendre, informatiques ou physiques, doit être proportionnelle aux risques qui pèsent sur les personnes en cas d'incident.
- Des réflexes doivent être mis en place : mises à jour des antivirus et logiciels, changement régulier des mots de passe complexes, ou chiffrement des données dans certaines situations. En cas de perte ou de vol d'un outil informatique, il sera plus difficile pour un tiers d'y accéder.

Quels sont les droits des Personnes physiques en matière de protection des données personnelles ?

1 - Les personnes physiques peuvent obtenir des informations sur la nature, l'origine et l'usage des données personnelles qui les concernent. En cas de transmission de leurs données personnelles à des tiers, les personnes physiques peuvent également obtenir des informations concernant l'identité des destinataires.

2 - Droit de rectification : les personnes physiques peuvent demander que des données personnelles inexactes ou incomplètes soient rectifiées ou complétées.

3 - Droit à l'effacement : les personnes physiques peuvent demander l'effacement de leurs données personnelles. Le responsable de traitement devra procéder à l'effacement des données dans les meilleurs délais, sauf dans les cas prévus par la réglementation, en particulier si les données personnelles sont traitées pour respecter une obligation légale ou réglementaire. Il est à noter dans ce cas que la personne physique ne pourra plus prétendre aux prestations de l'ASSOCIATION SNEMM, l'association étant alors incapable de répondre aux obligations réglementaires auxquelles il est lui-même soumis.

4. Droit d'opposition : les personnes physiques peuvent s'opposer à certains traitements de leurs données personnelles pour des raisons tenant à leur situation particulière sauf s'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts, droits et libertés fondamentales de la personne physique. Si le droit d'opposition est exercé par la personne physique, celui-ci ne pourra plus prétendre aux prestations de l'association SNEMM, l'association étant alors incapable de répondre aux obligations réglementaires auxquelles elle est elle-même soumise.

5. Droit à la portabilité : les personnes physiques peuvent accéder aux données personnelles les concernant. Ce droit à la portabilité ne peut s'exercer que lorsque le traitement de données personnelles est opéré à la suite du consentement de la personne physique, ou pour les besoins de l'exécution d'un traitement.

Pour exercer ces droits, les personnes physiques doivent d'adresser à la personne en charge du traitement des données : le délégué à la protection des données - le DPD.

Application du RGPD par les sections et les unions départementales.

Pas de registre pour les sections et les unions départementales.

Cependant elles doivent observer les grands principes imposés au siège :

- ✓ Ne recueillir que les données utiles ;
- ✓ Obtenir le consentement des personnes ;
- ✓ Assurer la protection et la sécurisation des données que ce soit sur papier ou surtout sur ordinateur (piratage) ;
- ✓ Observer la durée de conservation (archivage) ;
- ✓ Respecter de la chartre de la SNEMM qui sera prochainement diffusée.