NOTE

DATE 17 décembre 2018 OBJET RGPD

EXPÉDITEUR MSI/Service juridique

DESTINATAIRE(S)
Comités régionaux et départementaux
Copie : CODIR, Direction, ATP, PAF

Note sur le Règlement Général sur la Protection des Données (RGPD)

Le règlement général sur la protection des données personnelles (RGPD), mis en place en mai 2018, a instauré de nouvelles obligations à l'égard des structures qui collectent des données personnelles. En France, c'est la Commission Nationale de l'Informatique et des Libertés (CNIL) qui est chargée d'accompagner et de contrôler la mise en place de ce nouveau règlement européen. La FFRandonnée est concernée à tous les niveaux (National, Comités, Clubs).

Le RGPD renforce la responsabilité des organismes concernés. L'ancien régime juridique en vigueur sur les données personnelles (loi de 1978) était un système déclaratif. Aujourd'hui, on se situe davantage dans un système d'autocontrôle et de sanctions. Cependant, il faut noter que les associations ne sont pas les premières « cibles » du RGPD. En cas de contrôle, il s'agira surtout de montrer la bonne foi de nos structures et que les démarches de mise en conformité ont été entreprises.

Au-delà du contrôle qui pourrait être fait, la mise en place du RGPD doit être l'occasion de revoir nos outils informatiques, nos procédures : les données que l'on enregistre sur les personnes sont-elles toutes légitimes en regard de nos besoins ? A-t-on bien sécurisé leur accès pour qu'elles ne soient pas divulguées indûment ? Comment traite-t-on les demandes de désinscription, de suppression ? etc.

Qu'est-ce qu'une donnée personnelle ?

La CNIL (qui a adapté les définitions issues du règlement européen) considère une donnée personnelle comme « *toute information identifiant directement ou indirectement une personne physique* ». Il peut ainsi s'agir d'un nom, prénom, numéro de téléphone, date de naissance, adresse… Une personne est considérée comme identifiée lorsqu'elle apparait dans un fichier. Il convient ainsi de faire preuve de vigilance : certaines données, qui a première vue pourraient paraitre comme anonymes, pourraient en fait constituer des données personnelles (ex : combinaison de données qui, recoupées ensemble, permettent d'identifier une personne).

Attention : Eviter de traiter des données sensibles sur les personnes (origine raciale, ethnique, opinions politiques, philosophiques, religieuses, appartenance syndicale, santé,

vie sexuelle, numéro de sécurité sociale). A noter que le certificat médical obligatoire pour toute prise de licence n'est pas considéré comme une donnée sensible.

Qu'est-ce que le traitement des données ?

Selon la CNIL, il s'agit de « *toute opération portant sur des données personnelles, quel que soit le procédé utilisé* ». Parmi les procédés utilisés, on peut citer la collecte, l'enregistrement, la conservation, l'extraction, la communication par diffusion…

La vie fédérale est source de traitement de nombreuses données personnelles : lors de la prise de licence, lors de l'inscription à une sortie de randonnée, à un séjour ou voyage… On retrouve ici les fichiers de membres des associations (qui contiennent donc des données personnelles), votre annuaire de membres du comité directeur avec les adresses et téléphones personnes, les fichiers destinés aux newsletters, aux salariés…

Quels sont les grands principes du traitement de données ?

Le RGPD établit une liste de principes à respecter lorsqu'on collecte des données personnelles. Ces principes sont extraits directement du règlement européen :

(1) Elles doivent être traitées de manière licite, loyale et transparente vis-à-vis de la personne concernée.
(2) Elles doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités. En d'autres termes, la collecte des données personnelles doit toujours obéir à un but précis, et vous devez être capable de définir ce but.
(3) Elles doivent être adéquates, pertinentes, et limitées à ce qui est nécessaire au regard du but recherché. Vous ne devez collecter que les données dont vous avez strictement besoin.
(4) Elles doivent être exactes, et si nécessaire, tenues à jour. Il existe un droit de rectification et de suppression des données inexactes.
(5) Elles doivent être conservées sous une forme permettant l'identification des personnes pendant une durée n'excédant pas celle nécessaire au but recherché. Vous devez effacer les données de la personne lorsque celles-ci ne répondent plus au but initial.
(6) Elles doivent être traitées de façon à garantir leur sécurité à tout moment (protection contre le vol, la perte, la destruction…). En effet, l'association est juridiquement responsable des moyens mis en œuvre pour protéger les données personnelles. Cette responsabilité a été renforcée par le RGPD, et les structures devront assurer à tout moment une protection optimale des données personnelles collectées, et être en mesure de le démontrer. L'accès à ces données doit être limité au strict nécessaire.

Quels sont les motifs de traitements de données autorisés ?

Il y a 6 conditions possibles pour que le traitement d'une donnée personnelle soit légal :

a) La personne a consenti au traitement de ses données pour une ou plusieurs finalités spécifiques ;
b) Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
c) Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie prenante ;

d) Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
e) Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ;
f) Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers.

Par exemple, pour le réseau fédéral, on peut s'appuyer sur la condition c) : le traitement de certaines données est nécessaire à l'exécution du contrat d'association entre la structure et ses adhérents.

Quels droits ont les personnes dont les données ont été collectées ?

Il s'agit là d'un pan essentiel du RGPD. Il a renforcé les droits des personnes sur leurs données collectées. Le RGPD permet à l'utilisateur d'avoir la main sur la gestion de ses données personnelles : il doit pouvoir, à tout moment, décider de l'usage des données qui ont été collectées, directement ou indirectement. Il s'agira donc d'organiser le cycle de vie des données personnelles collectées pour permettre à la personne d'exercer ses droits lorsqu'elle le souhaite. On distingue trois applications : droit à l'information, droit d'accès à ses données personnelles et droit de rectification et suppression.

Le National accompagne le réseau fédéral dans la prise en compte de ces nouvelles obligations. Cependant, il est important de noter que le traitement des données personnelles est l'affaire de tous.

Quelles responsabilités des comités vis-à-vis des données enregistrées dans les systèmes informatiques fédéraux ?

On parle ici des données sur les personnes enregistrées premièrement dans le système de gestion de la vie fédérale (SGVF), utilisées par d'autres systèmes fédéraux (outil de gestion des formations, d'envoi de newsletter…). Cela comprend pour chaque personne leur : nom, prénom, date de naissance, adresse postale, numéro de téléphone, adresse e-mail, numéro unique (d'adhésion ou autre donnée à toute personne dans le SGVF).
Pour répondre aux demandes des personnes sur ces données, le National a mis en place une adresse donneespersonnelles@ffrandonnee.fr, mentionnée sur les sites fédéraux du national, et sur laquelle vous pouvez renvoyer des questions qui vous seraient remontées par les personnes.

Recueil du consentement à l'utilisation des données
En tant que représentants locaux de la Fédération, relais auprès des clubs, acteurs directs de la collecte (nouvelles licences comités), vous participez à l'alimentation du SGVF.
Le SGVF prévoit actuellement le consentement des personnes sur :
- L'acceptation de recevoir des informations de la FFRandonnée (envoi de newsletters, questionnaires)
- L'acceptation de recevoir des informations des partenaires de la FFRandonnée.

Ces consentements apparaissent sous une forme « opt-in » : il faut faire une action de cocher la case pour recevoir des informations, plutôt que d'avoir à faire une action pour ne pas recevoir (mode « opt-out »).
Vous devez vous assurer que le consentement des personnes est bien recueilli en mode « opt-in » par les clubs avant d'ajouter ces personnes au SGVF.

Utilisation des données présentes dans le SGVF

Vous pouvez extraire du SGVF la liste de vos membres, les adhérents du comité départemental ou du comité régional et ensuite utiliser ces extractions pour alimenter un outil d'envoi de newsletters, des statistiques particulières…

A partir de ces extractions, vous devez veiller :

- A respecter le consentement exprimé par la personne : ne pas envoyer de newsletter du Comité à quelqu'un qui ne souhaite pas recevoir d'informations de la Fédération (information figurant dans le SGVF, pour chaque licencié) ;
- A sécuriser les fichiers extraits pour éviter que les données personnelles qui y sont contenues ne soient divulguées à tort : s'assurer que tout stockage ou envoi par messagerie de ces fichiers soit à minima protégé par un mot de passe. Pour cela, nous vous recommandons d'utiliser l'outil fédéral de partage de fichiers One Drive.
- A utiliser des outils ou services exploitant ces données « conformes au RGPD ».

Violation des données

Si vous constatez une violation de données (par exemple : perte d'une clé USB contenant un fichier d'adhérents non protégé par un mot de passe, modifications inexpliquées de données personnelles remontées par les clubs), vous devez en informer le National (boîte donneespersonnelles@ffrandonnee.fr) qui appréciera la situation et vous orientera sur les suites à donner le cas échéant auprès des personnes concernées et de la CNIL..

Quelles responsabilités des comités vis-à-vis des données et traitements mis en œuvre en plus des systèmes fédéraux ?

Il arrive que vous mettiez en place des traitements informatiques de données personnelles pour votre propre compte : systèmes d'inscription à des manifestations, des envois de newsletters, etc., généralement par utilisation de services en ligne prêts à l'emploi.

Vous avez également à gérer les données de vos salariés (on fait référence ici à des systèmes de gestion automatisés de paie, de congés, de carrière).

Enfin, vous pouvez être amenés à collecter sur les personnes davantage de données personnelles qu'il n'y en a dans le SGVF.

Pour tous ces traitements propres aux Comités, il faut mettre en œuvre essentiellement les dispositions suivantes :

(1) Mettre en place un registre des traitements : un modèle[1] est disponible sur le site de la CNIL, l'établissement de ce registre doit être l'occasion de vérifier que les données personnelles collectées sont bien légitimes au regard des finalités du traitement.

(2) S'assurer que les fournisseurs de logiciels, de solutions en ligne, d'hébergement respectent bien le RGPD : ces tiers ont un rôle bien défini par le RGPD, celui de sous-traitant ; les fournisseurs reconnus du marché affichent désormais tous sur leur site les dispositions qu'ils mettent en œuvre, par exemple le fait qu'ils hébergent les données sur des serveurs en Europe, voire les incluent dans les contrats (autrement dit, si un fournisseur de service n'indique pas clairement sur son site les dispositions mises en œuvre dans le cadre du RGPD, il est à bannir) .

(3) S'assurer que le consentement à l'utilisation des données a bien été recueilli en mode « opt-in » pour tous les traitements : par exemple, si vous organisez une manifestation « grand public » et que vous récupérez les adresses méls des

[1] https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.rtf

personnes inscrites, vous ne pouvez les injecter dans votre outil de newsletter que si le consentement a été recueilli lors de l'inscription.

(4) Sécuriser ses propres moyens informatiques : à minima protéger l'accès aux PC et à l'infrastructure réseau et serveur du comité par des mots de passe suffisamment élaborés et complexes (mélangeant nombres, caractères majuscules et minuscules et symbole) et fréquemment renouvelés.

(5) Prévoir une procédure de désabonnement des newsletters (tous les fournisseurs de telles solutions en ligne en ont normalement une)

(6) Prévoir une procédure de prise en compte des demandes d'information accès, rectification et suppression de données personnelles pour tout ce qui n'est pas directement issu du SGVF, cela passe notamment par l'affichage sur le site web du Comité d'une boîte mél permettant d'envoyer une telle demande (typiquement la boîte générique departement@ffrandonnee.fr ou region@ffrandonnee.fr , la création d'une boîte ad-hoc n'est pas nécessaire au vu de la volumétrie attendue de tels messages).

(7) Prendre systématiquement l'habitude de mettre en copie cachée (Cci) vos mails envoyés à de multiples destinataires pour éviter de divulguer vos répertoires d'adresses mails.

Sources :

- *Règlement général sur la protection des données n°2016/679 consultable à l'adresse suivante : https://www.cnil.fr/fr/reglement-europeen-protection-donnees*
- *Dossier sur le RGPD sur le site de la CNIL : https://www.cnil.fr*