Département Administration
Commission Juridique

Février 2018

Application du RGPD (Règlement Général sur la Protection des Données) à la FFAB

Jusqu'à présent en France, la protection des données individuelles (pour les personnes physiques uniquement) était organisée par la loi du 06/01/1978 (dite « Informatique et Liberté »), avec comme autorité de contrôle la CNIL (Commission Nationale Informatique et Liberté).
Les traitements de données devaient faire l'objet d'une déclaration afin que la CNIL vérifie leur légalité (N.B. : constitue un « traitement » toute manipulation de données, qu'elles soient analysées ou non).

Les **associations comme la FFAB étaient dispensées de déclaration** des fichiers qu'elles élaboraient, lorsque ces fichiers étaient strictement nécessaires au fonctionnement de l'association.
Toute personne avait droit de demander la consultation et la modification (voire suppression) de ses données personnelles), et chacun devait être informé de ce droit.

L'adoption du règlement européen 2016/679 dit « RGPD », **applicable directement dans les Etats-membres au 25/05/2018** (et donc sans transposition nécessaire dans le droit national à la différence de la très grande majorité des directives), à lire ensemble avec la directive 95/46 sur le même sujet, apporte des modifications dans cet état du droit qui seront présentées ci-après et mises en perspectives dans le cadre de l'activité de la Fédération.

I. LES GRANDES LIGNES DU RGPD

Le RGPD implique d'une part que les obligations des détenteurs de fichiers (qu'ils soient informatisés ou manuels) soient renforcées, tout comme le droit des personnes dont les données sont collectées et conservées.

1. Renforcement des obligations des détenteurs de fichiers et extension aux associations

Le dispositif du RGPD s'applique à tout détenteur de fichiers de données personnelles, et notamment **à toute association**.

Il repose sur le développement d'un **auto-contrôle renforcé**, et impose des déclarations auprès des autorités (CNIL en France) en cas de traitement de données très sensibles, ou de perte, destruction et/ou vol des données conservées.

Pour ce faire :

- *un examen complet/recensement des traitements existants* est nécessaire avec l'établissement d'un registre de ces traitements ;
- *l'examen permettra d'identifier ceux qui peuvent poser problème* au vu de la règlementation et les mettre en conformité :
    - les données à collecter doivent répondre à l'intérêt légitime d'un responsable de traitement et être « adéquates, pertinentes et limitées à ce qui est nécessaire pour les finalité pour lesquelles elles sont traitées » ;
    - une évaluation doit être faite sur les données collectées, la base juridique de leur collecte et les modalités du consentement recueilli, les acteurs y ayant accès pour traitement et/ou consultation, les objectifs du traitement ;
    - les données sensibles doivent faire l'objet d'une étude d'impact pour évaluer cet intérêt légitime et prendre les mesures nécessaires en conséquence en terme de protection (voire de déclaration auprès de l'autorité compétente) : ces données sensibles, d'après le RGPD et la CNIL, comprennent au moins les données révélant l'origine raciale ou ethnique, les opinions politiques, religieuses ou philosophiques, les orientations sexuelles et la situation familiale, les adhésions syndicales, les données biométriques et informations relatives à la santé ; on peut y ajouter les coordonnées bancaires et numéro de sécurité sociale, ainsi que les infractions et condamnations ;
    - une durée de conservation doit exister et correspondre au strict minimum nécessaire ;
- *la remise à plat des procédures internes voire des formulaires de demandes d'informations permettant la collecte des données* est à réaliser pour vérifier que l'ensemble des intervenants sur le traitement soit informé de la bonne conduite à tenir et s'engage sur la confidentialité des données traitées ;
- *une information générale* est conseillée afin que les personnes concernées (autant les personnes ayant accès aux données que les personnes dont les données sont collectées) puissent avoir connaissance des droits et obligations de base en la matière.

En outre, le règlement impose de **renforcer les contrats existants** avec les hébergeurs, les routeurs et tous les prestataires (+ sous-traitants) ayant accès aux données afin d'insérer des mentions obligatoires relatives à la sécurité des données (en particulier le chiffrement des données et l'existence de procédures de sécurisation de celle-ci), si ces mentions n'existent pas déjà.

Un délégué à la protection des données peut être désigné (obligatoire dans certains cas) afin de superviser l'ensemble de ces éléments et être le référent sur le sujet.

2. Renforcement du droit des personnes

Le RGPD confirme et renforce le droit de personnes dont les données sont collectées, avec notamment :

- nécessité, en application du principe de transparence, d'un *consentement recueilli de manière « libre, spécifique, éclairée et non univoque » et surtout par un « acte positif clair »* (donc pas de case précochée ou de silence qui vaudrait acceptation) : il peut se manifester par écrit (y compris électroniquement) ou par oral (mais il faut être capable de démontrer qu'il a bien été recueilli…) ;
- nécessité pour ce faire *d'informer clairement la personne sur la finalité du traitement ainsi que sur le droit à modification, réclamation, rectification des données*, ainsi que la *durée* de conservation de celles-ci (droit à l'oubli) ; il convient de noter :
    - que l'information peut être réalisée par voie électronique ;
    - que les demandes de modification ou de suppression des données doivent pouvoir être faites par voie électronique, et que le responsable du traitement doit pouvoir y répondre dans un délai d'un mois maximum ;
- *droit d'être informée en cas de vol des données*, si un « risque élevé » pour ses droits et libertés existe.

II. L'APPLICATION DU RGPD A LA FFAB

II.1. BILANS A REALISER

1. Recensement des traitements existants et des données collectées

La FFAB doit réaliser la cartographie des traitements existants dans la structure et analyser le risque lié à ceux-ci.
Les questions à se poser sont les suivantes :

	Traitement 1	Traitement 2 le cas échéant	Etc…
1. Quel(s) traitement(s) existe(nt) ?			
2. Quelles sont les données traitées ?			
3. Quel est l'objectif du traitement ?			
4. Existe-t-il des données sensibles dans ce(s) traitement(s) ?			
5. Les données sont-elles strictement nécessaires à la finalité du traitement ?			
6. Qui traite ces données : - en interne (en saisie et/ou en accès consultation) ; - et en externe (saisie, consultation, accès, modification…) : prestataires et sous-traitants.			
7. Flux des données (transferts intra-UE ou transferts de données hors de l'UE).			
8. Comment sont-elles collectées : - pour l'intérêt légitime de l'association ? - par contrat (signature licence) ? - par recensements divers ? - le consentement des personnes est-il clair sur la collecte et l'utilisation qui sera faite des données ?			
9. Existe-t-il une durée de conservation des données et si oui quelle est-elle avant destruction ?			

2. Recensement de nos procédures relatives aux traitements des données

Une fois l'identification du ou des traitements réalisés, les questions à se poser sont également les suivantes pour prioriser ensuite les actions à mener :

❖ **Information des personnes dont les données sont collectées** :

- le consentement est-il donné de manière active et claire, avec la connaissance de la finalité de la collecte des données ainsi que la durée de leur conservation ?
- toute personne sait-elle qu'elle a droit à la communication des données la concernant ainsi qu'un droit à rectification et suppression ?

❖ Quel est le niveau de sécurité d'accès et le niveau d'information sur la **sécurité et de confidentialité des données** pour les acteurs internes et externes ayant accès à celles-ci ? S'engagent-ils sur cette confidentialité et sur la **non-réutilisation à d'autres fins** que celles de leur collecte, ainsi que sur une possibilité ou non de communication des fichiers à d'autres structures y compris externes à la fédération ? Les acteurs concernés étant :
- personnel fédéral et bénévoles ayant accès aux fichiers en saisie et/ou modification ;
- responsables de clubs (pour la partie licences en ligne et accès aux espaces réservés) ;

- responsables des structures (Ligues, Délégations, CID et CODEP) qui ont accès aux fichiers via les espaces réservés ;
- prestataires informatiques et hébergeurs + leurs sous-traitants éventuels.

❖ **Des procédures formalisées** sont-elles mises en place :

- pour communiquer, modifier ou supprimer des données à la demande des personnes concernées (avec une information de celles-ci à ce sujet) ;
- pour supprimer les données à la fin de la durée de conservation de celle-ci (de manière automatique ou manuellement) ;
- pour alerter l'autorité compétente dans les 72 heures (CNIL) en cas de vol de données, perte, destruction, piratage etc., ainsi que pour informer les personnes concernées dans les meilleurs délais si cela présente un risque « grave » pour leurs droits et libertés.

II.2. ACTIONS A ENVISAGER D'ICI FIN MAI 2018

1. Création d'un registre identifiant les traitements

Le registre n'est pas obligatoire pour les structures de moins de 250 employés, mais il est toutefois recommandé car il constitue une aide utile dans le recensement des traitements.

La CNIL propose un modèle téléchargeable en format Excel (https://www.cnil.fr/sites/default/files/atoms/files/registre-reglement-publie.xlsx), qui se présente ainsi :

Onglet 1

	Identification du traitement				Acteurs	Finalité du traitement	Transferts hors UE ?	Données sensibles ?
	Nom / sigle	N° / REF	Date de création	Dernière mise à jour	Responsable du traitement	Finalité principale	Oui /non	Oui/non
3								
4								
5								
6								
7								
8								
9								

Onglet 2

43	Numéro d'identification national unique (NIR pour la France)					
44						
45	Catégories de personnes concernées	Description				
46	Catégorie de personnes 1					
47	Catégorie de personnes 2					
48						
49	Destinataires	Description	Type de destinataire			
50	Destinataire 1					
51	Destinataire 2					
52	Destinataire 3					
53	Destinataire 4					
54						
55	Tranferts hors UE	Destinataire	Pays	Type de Garanties		Lien vers le doc
56	Organisme destinataire 1					
57	Organisme destinataire 2					
58	Organisme destinataire 3					
59	Organisme destinataire 4					
60						

Pour rappel, l'article 30 de la directive 95/46 précise le contenu du registre :
1. Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes :
a) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;
b) les finalités du traitement ;
c) une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;

e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49 § 1, 2e alinéa, les documents attestant de l'existence de garanties appropriées ;
f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;
g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, § 1.
2. Chaque sous-traitant et, le cas échéant, le représentant du sous-traitant tiennent un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant :
a) le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles du délégué à la protection des données ;
b) les catégories de traitements effectués pour le compte de chaque responsable du traitement ;
c) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49,§ 1, 2e alinéa, les documents attestant de l'existence de garanties appropriées ;
d) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, § 1.

2. Analyse des données collectées et actions à mener

L'identification des données collectées réalisé lors de la cartographie (cf. ci-dessus) et notamment les réponses aux questions des points 2 à 5 doivent permettre de lister :

- les données qu'il convient de **continuer à collecter** ;
- les données qu'il convient de **supprimer des fichiers et des formulaires** qui les contiennent ;
- les données sensibles qu'il faut soumettre à **étude d'impact** (« PIA » ou « Privacy Impact Assessment ») : à ce stade, compte-tenu de la nature des informations que la Fédération collecte, il ne semble pas qu'il y ait de données sensibles nécessitant une telle étude d'impact dans les fichiers fédéraux (aucune information de ce type n'est demandée à part la date du certificat médical – qui n'est pas un élément de santé et ne préjuge pas des pathologies éventuelles du licencié).

3. Gestion des contrats avec le(s) prestataire(s) et éventuel(s) sous-traitant(s)

Les contrats avec les prestataires doivent être relus et le cas échéant complétés par des mentions relatives à la sécurité des données (cryptage, procédures de destruction en fin de contrat, procédures en cas de piratage, vol ou destruction des données, etc.).

Pour les prestataires, on peut renvoyer aux clauses contractuelles types de la Commission Européenne, distinctes selon que les données soient transférées ou non hors de l'UE.
Pour les sous-traitants, les mentions figurent à l'article 28 du RGPD :

[…] le sous-traitant:
a) ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis; dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;
b) veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
c) prend toutes les mesures requises en vertu de l'article 32 ;
d) respecte les conditions visées aux paragraphes 2 et 4 pour recruter un autre sous-traitant ;
e) tient compte de la nature du traitement, aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au chapitre III ;
f) aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ;
g) selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel ; et
h) met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.
En ce qui concerne le point h) du premier alinéa, le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du présent règlement ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

4. Mise en place de l'information/formation

❶ INFORMATION ET CONSENTEMENT DES LICENCIES AU RECUEIL DES DONNEES

Lors la souscription de la licence (ou de toute inscription à une formation, grade, ou stage dont les données feraient ensuite l'objet d'un traitement), il convient que la personne fournissant ses données personnelles :

- soit informée des éléments suivants :
  - que les données collectées seront traitées pour la gestion du fichier des licenciés (ou trouver une autre formulation plus adéquate à la finalité du ou des traitements effectués) ;
  - que ces données peuvent être modifiées ou supprimées à sa demande par tout moyen écrit adressé au siège fédéral à tout moment, et qu'elles seront supprimées au bout d'un délai de XX années ;
- puisse établir clairement qu'elle consent à leur traitement pour la finalité indiquée.

Matériellement :

- pour les documents papiers, cela reviendrait à ajouter une mention sur le document ou la signature vaut consentement ;
- pour les documents en ligne (notamment les licences), une colonne avec une case à cocher sur le sujet (avec une mention claire établie sur la feuille en haut ou en bas) permettrait de recueillir le consentement, de la même manière que le licencié reconnaît avoir été informé des dispositions relatives aux assurances.

La CNIL conseille la mention suivante (les mentions surlignées en jaune peuvent être modifiées)

Les informations recueillies sur ce formulaire sont enregistrées dans un fichier informatisé par **Fédération Française d'Aïkido et de Budo (FFAB)** pour **la gestion du fichier des licenciés.**
Elles sont conservées pendant **5 ans à compter de la fin de la saison de la dernière licence souscrite** et sont destinées **à l'usage exclusif de la FFAB.**
Conformément à la loi, vous pouvez exercer votre droit d'accès aux données vous concernant et les faire rectifier ou supprimer en contactant : **ffab.aikido@wanadoo.fr ou FFAB - Les Allées - 83149 BRAS**

❷ INFORMATION ET ENGAGEMENT DES EMPLOYES, BENEVOLES ET RESPONSABLES DES STRUCTURES AYANT ACCES AU TRAITEMENT DES DONNEES (SAISIE ET/OU CONSULTATION)

Toute personne ayant accès aux données personnelles fournies par les licenciées doivent pouvoir être informées :

- de leur caractère confidentiel ;
- de l'obligation de respecter la finalité pour laquelle elles ont été collectées : il ne doit pas leur être permis de faire d'autres utilisations, ni d'autoriser des cessions à quiconque ou transmission sans autorisation de la ou des personne(s) concernée(s).

Dans ce cadre, il paraît indispensable que chaque personne ayant accès à ces données (salariée ou bénévole dans le cadre des structures pouvant éditer les états, par exemple) signe un engagement relatif au respect de cette confidentialité et de l'utilisation exclusive du fichier en interne et pour la seule finalité pour laquelle les données ont été recueillies.
En outre, ce document prévoirait que toute personne ayant eu connaissance d'un piratage de son compte ou d'une suspicion de vol ou destruction de données le signale dans un délai (maximum 72 heures) à la Fédération.

Enfin, les gestionnaires des licences (en général le président ou le secrétaire) au sein des clubs doivent être informés de l'obligation de conserver les fiches de demandes de licences (papier ou tableau récapitulatif pour les licences en ligne) puisqu'il s'agit du seul document permettant de prouver que le consentement a été donné de manière expresse et éclairé.

❸ INFORMATION ET AVERTISSEMENTS AUX RESPONSABLES DES CLUBS ET STRUCTURES

Prévoir, dans les courriers clubs, une note d'information (une page maximum) sur le RGPD et les règles élémentaires à suivre pour se conformer à celui-ci, avec renvoi vers le site de la CNIL.

N.B. : la Fédération n'a pas d'obligation règlementaire d'information auprès de ses clubs, mais il est préférable d'y procéder, sachant qu'ensuite chaque structure y compris déconcentrée est responsable de ses propres traitements.

❹ PROCEDURE DE DEMANDE DE MODIFICATION OU DE SUPPRESSION DE DONNES

- introduire, sur tout support de demandes de données personnelles, une mention précisant que la personne peut solliciter, par tout moyen écrit adressé au siège fédéral, la modification ou la suppression des données personnelles la concernant ;
- prévoir qu'une réponse soit apportée dans le délai d'un mois maximum au demandeur.

❺ PROCEDURE DE SUPPRESSION DE DONNEES APRES DELAI DE CONSERVATION

- définir un délai de conservation pour chaque type de donnée ;
- organiser le mécanisme de suppression des données qui arrivent à expiration de leur délai de conservation :
    - suppression manuelle (avec quel type d'alerte afin de ne pas dépasser le délai) ?
    - nouveau service à définir avec le prestataire informatique ?

❻ PROCEDURE D'ALERTE EN CAS DE VOL, PERTE, DESTRUCTION OU PIRATAGE DE DONNEES

- mettre en place un mécanisme de détection de tout mouvement suspect sur les traitements des données avec le prestataire informatique (vol, perte, destruction accidentelle ou intentionnelle, piratage) ;
- formaliser un modèle de courrier d'alerte à la CNIL précisant la nature du mouvement intervenu, la date et l'heure (supposées si non connues avec exactitude) afin de pouvoir le remplir rapidement le cas échéant ;
- formaliser un modèle de courrier ou courriel d'information aux personnes concernées par ce type d'évènement si l'on estime qu'il existe un risque grave d'atteinte à leurs droits et libertés.

5. Création du dossier RGPD

Le dossier permettant de contrôler la conformité au règlement du dispositif mis en place par la Fédération devra se composer, comme l'indiquer le guide de la CNIL, des éléments suivants :

❖ **Documentation sur le(s) traitement(s) des données personnelles**

- le registre des traitements (pour les responsables de traitements) ou des catégories d'activités de traitements (pour les sous-traitants) ;
- les analyses d'impact sur la protection des données (PIA) pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes, ***s'ils ont été considérés comme nécessaires*** ;
- l'encadrement des transferts de données hors de l'Union européenne (notamment, les clauses contractuelles types, les BCR et certifications) ***si c'est le cas***.

❖ **L'information des personnes**

- les mentions d'information réalisés à l'attention des personnes dont les données sont collectées ;
- les modèles de recueil du consentement des personnes concernées ;
- les procédures mises en place pour l'exercice des droits.

❖ **Les contrats qui définissent les rôles et les responsabilités des acteurs**

- les contrats avec les sous-traitants ;
- les procédures internes en cas de violations de données ;
- les preuves que les personnes concernées ont donné leur consentement lorsque le traitement de leurs données repose sur cette base.

Site utile avec guides et fiches :
https://www.cnil.fr/fr/comprendre-le-reglement-europeen