Fédération des Centres sociaux et Socioculturels de France [FCSF]

RGPD et Centres sociaux
Foire aux questions

RGPD... Depuis le mois de mai, nous sommes assailli.e.s de mails de mise en conformité avec ce nouveau « Règlement Général sur la Protection des Données ». Mais qu'est-ce que c'est ?
Le RGPD est un règlement européen qui détaille les nouvelles obligations liées à l'utilisation des données personnelles. Celui-ci est décrit comme la plus grande avancée de ces 20 dernières années, concernant la législation sur les données personnelles et est entré en vigueur le 25 mai 2018.

Il s'applique aux acteurs économiques et sociaux, les entreprises bien sûr mais donc aussi les associations, les fondations, les administrations, les collectivités…et donc les centres sociaux !

Cette nouvelle directive est d'abord un grand pas en avant pour les citoyens en termes de respect et protection des données personnelles, et s'inscrit dans les valeurs que nous portons, dans les centres sociaux.

Alors, comment se mettre en conformité, même a minima ? Quelles mentions faire apparaître sur les bulletins d'inscription et d'adhésion, sur nos sites internet ? Quelles obligations respecter concernant les fichiers que nous gérons ?
Vous trouverez dans cette Foire aux questions, quelques premiers éléments de réponse, les plus simples possibles, élaborés par la Fédération des Deux Sèvres et la Fédération nationale.
Nous espérons que ce document vous sera utile pour votre centre.

Pour des informations plus détaillées, vous pourrez retrouver quelques ressources en fin de document.
C'est parti !

août 2018

Le cadre général

1. LE RGPD, QU'EST-CE QUE C'EST ?

Le « Règlement Général sur la Protection des Données » est un règlement européen qui détaille les nouvelles **obligations liées à l'utilisation des données personnelles**, entré en vigueur le 25 mai 2018.

Cette nouvelle directive est un grand pas en avant pour les citoyens : l'arrivée de ce règlement sonne la fin d'une période où la protection des données personnelles pouvait être facilement ignorée (de nombreux principes mais pas ou peu de sanction).

Toutes les organisations doivent entreprendre les démarches pour se mettre en conformité avec ce règlement (**y compris les centres sociaux** !!!)

2. UNE DONNÉE PERSONNELLE, C'EST QUOI ?

Le RGPD définit une donnée personnelle comme étant **« toute information se rapportant à une personne physique identifiée ou identifiable […] directement ou indirectement. »** Un simple nom est donc déjà une donnée personnelle. Adresse, date de naissance, mail, quotient familial…en sont d'autres que l'on utilise souvent dans les centres sociaux.

3. AVEC LE RGPD, QU'EST-CE QUI CHANGE ?

6 principales nouveautés sont apportées par le RGPD :

1 — Le renforcement des droits des personnes :

il impose de recueillir et conserver le consentement au traitement des données personnelles.

2 — L'obligation d'information :

les structures victimes d'un piratage de données personnelles doivent informer dans les 72 h la CNIL et les personnes dont les informations ont été volées.

3 — Des sanctions lourdes :

il met en place des sanctions dissuasives, allant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire d'une organisation. Le montant le plus élevé étant celui retenu.

4 — Le principe de minimisation des données collectées :

il impose de ne collecter que les renseignements strictement nécessaires au regard des finalités pour lesquelles elles sont traitées.

5 — Le droit de portabilité des données :

les personnes, dont les informations ont été collectées, ont le droit de demander à recevoir les données personnelles les concernant.

6 — Le registre des données :

il oblige les organisations à tracer l'ensemble des traitements des données personnelles mis en œuvre au sein de l'organisation.

Pas de panique !

Vous pouvez y aller progressivement. Certaines améliorations sont simples à mettre en place (mentions sur les formulaires et sites...), d'autres demandent plus de temps...

Un enjeu : lancez le travail, à la mesure de vos moyens !

4. COMMENT SE METTRE EN CONFORMITÉ ?

La CNIL propose de le faire en 4 étapes, reprises ci après :

Constituez un registre de vos traitement de données : Identifiez les activités principales de votre structure qui nécessitent la collecte et le traitement de données (Exemples : recrutement, gestion de la paie, gestion des inscriptions, des adhésions...). Le registre est placé sous la responsabilité du dirigeant de l'organisation.
Pour avoir un registre le plus complet et à jour, il faut en discuter et être en contact avec toutes les personnes de la structure susceptibles de traiter des données personnelles.

Pour vous aider : appuyez-vous sur le modèle de registre : voir question 5

Faites le tri dans vos données : A cette occasion, améliorez vos pratiques ! Minimisez la collecte de données, en éliminant de vos formulaires et vos bases de données toutes les informations inutiles.
Redéfinissez qui doit pouvoir accéder à quelles données dans votre structure. Pensez à poser des règles automatiques d'effacement ou d'archivage au bout d'une certaine durée dans vos applications.

Respectez les droits des personnes : A chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information, notamment :

- pourquoi vous collectez les données (« la finalité » ; par exemple pour diffuser une lettre d'information, pour gérer la mise en place et l'animation d'une activité) ;
- ce qui vous autorise à traiter ces données (le « fondement juridique » : il peut s'agir du consentement de la personne concernée, de l'exécution d'un contrat, du respect d'une obligation légale qui s'impose à vous, de votre « intérêt légitime ») ;
- Qui a accès aux données ;
- Combien de temps vous les conservez (exemple : « 5 ans après la fin de l'activité ») ;
- Les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits (par un message sur une adresse email dédiée, par un courrier postal) ;

-> exemples de mentions d'informations sur le site du CNRS : www.cil.cnrs.fr/CIL/spip.php?rubrique421

Sécurisez vos données : Si le risque zéro n'existe pas en informatique, vous devez prendre les mesures nécessaires pour garantir au mieux la sécurité des données. Vous êtes en effet tenu à une obligation légale d'assurer la sécurité des données personnelles que vous détenez. Les mesures à prendre, informatiques ou physiques, dépendent de la sensibilité des données que vous traitez et des risques qui pèsent sur les personnes en cas d'incident.
Des réflexes doivent être mis en place : mises à jour de vos antivirus et logiciels, changement régulier des mots de passe et utilisation de mots de passe complexes...

5. COMMENT TENIR UN REGISTRE DE TRAITEMENT DES DONNÉES ?

L'idée ? Mettre en place, en interne, une documentation complète, tenue à jour, qui atteste que vous êtes en conformité avec le RGPD. **Une cartographie des données pour montrer patte blanche, en somme.** Votre registre doit répondre à trois questions-phares :

- **Qui ?** Listez les personnes en interne amenées à traiter des données et le cas échéant, vos sous-traitants en vous assurant qu'ils sont aussi dans une démarche de mise en conformité au RGPD et en prévoyant de réviser vos contrats ;
- **Quoi ?** Cartographier les traitements de données personnelles réalisées par votre structure (type de données collectées, finalités des traitements, preuve des consentements recueillis, informations portées à la connaissance des personnes concernées...) ;
- **Comment ?** Vérifier comment ces données sont traitées (transfert à l'étranger ou non, archivage ou suppression de données, etc.) et quelles mesures de sécurité sont mises en place en interne.

Pour votre registre, vous pouvez vous inspirer du modèle de registre sur le site de la CNIL.

Vous pouvez aussi télécharger des modèles de registres pré-remplis (centre social ou fédération). Il vous suffira de vérifier ou / et compléter les informations surlignées en jaune.

Pour télécharger le modèle de registre fédérations **cliquez ici** et le modèle registre centres sociaux, **cliquez ici**.

6. QUELLES SONT MES OBLIGATIONS VIS-À-VIS DE MES MEMBRES ?

Le consentement de la personne dont les données sont enregistrées dans un fichier n'est pas nécessaire lorsque ces données sont collectées dans le cadre de l'exécution d'un contrat, du respect d'une obligation légale, d'une mission d'intérêt public ou de votre intérêt légitime. En dehors de ces cas, le consentement de la personne concernée est obligatoire, il doit être explicite. C'est le consentement qui confère alors au fichier projeté son caractère licite. **Attention, même si le consentement n'est pas obligatoire, vous devez informer vos membres du traitement de leurs données**.

Exemple : « Les informations recueillies sont nécessaires pour votre adhésion. Elles font l'objet d'un traitement informatique et sont destinées à la comptabilité du centre social. En application des articles 39 et suivants de la loi du 6 janvier 1978 modifiée, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser à …… [indiquez-ici le service en charge de traiter les demandes] »

7. COMMENT OBTENIR LES CONSENTEMENTS EXPLICITES ?

Pour cela, il faut rédiger un texte de demande de consentement (nous reprenons ici une recommandation du guide Verticalsoft de janvier 2018 disponible en ligne) :

Exemple : « En adhérant à l'association et / ou en en remplissant ce formulaire d'inscription..., vous acceptez que l'Association XYZ mémorise et utilise vos données personnelles collectées dans ce formulaire dans le but d'améliorer votre expérience et vos interactions avec elle. En l'occurrence, vous autorisez l'Association XYZ à communiquer occasionnellement avec vous si elle le juge nécessaire afin de vous apporter des informations complémentaires sur ses projets et appels à dons via les coordonnées collectées dans le formulaire.
Afin de protéger la confidentialité de vos données personnelles, Association XYZ s'engage à ne pas divulguer, ne pas transmettre, ni partager vos données personnelles avec d'autres entités, entreprises ou organismes, quels qu'ils soient, conformément au Règlement Général de Protection des Données de 2018 sur la protection des données personnelles et à notre politique de protection des données ».

8. QUE DOIS-JE FAIRE POUR MES NEWSLETTERS ?

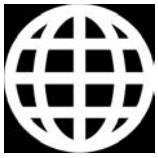
Pour les newsletters, vous devez vous assurer du consentement explicite des personnes inscrites sur la mailing list pour l'utilisation de leurs données. Le silence n'est pas un consentement. Une case précochée n'est pas un consentement. Il faut avoir la trace des personnes qui s'inscrivent à la newsletter, avoir la preuve qu'on n'a pas ajouté soi-même les mails dans la liste. Pour toute newsletter, il faut mentionner clairement qu'ils peuvent se désinscrire à tout moment. Et à l'inscription, mentionner à quoi servira leur adresse mail.

Exemple : « Votre adresse de messagerie est uniquement utilisée pour vous envoyer notre lettre d'information. Vous pouvez à tout moment utiliser le lien de désabonnement intégré dans la newsletter. »

9. QUE DOIS-JE FAIRE POUR MON SITE WEB ?

Votre site doit comporter une page de politique de confidentialité. Elle doit désormais expliquer concrètement ce que vous faites avec ces données. Faites-y apparaître :

- Vos coordonnées, ainsi que l'éditeur du site, et son hébergeur ;
- Quel type de données vous récoltez lors de la navigation sur votre site web : noms, prénoms, email, téléphone, adresse postale, adresse IP…;
- Pourquoi vous collectez ces données : communication par newsletter... ;
- Combien de temps vous stockez ces données ;
- Les mesures de sécurité que vous avez mises en place pour assurer la protection de ces données, ainsi que la manière dont ils peuvent exercer leur droit de modification ou de suppression de ces données.



Si vous êtes sur Wordpress, vous pouvez créer votre page de Politique de Confidentialité directement depuis l'onglet « Réglages » de votre interface WordPress. Y seront proposés des paragraphes prérédigés, optimisés pour le RGPD : à vous de sélectionner ceux qui concernent votre site.
Si votre site n'utilise pas Wordpress, vous pouvez vous inspirer de ce texte, en modifiant les informations qui concernent votre structure : http://www.centres-sociaux.fr/politique-de-confidentialite/

Questions plus spécifiques

10. LES DONNÉES SENSIBLES C'EST QUOI DANS LES CENTRES SOCIAUX ?

Définition de la CNIL : *« Information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes. »* Le numéro de sécurité sociale fait également partie des données considérées comme sensibles.

Dans les centres sociaux, des informations relatives à la vaccination des enfants peuvent être demandées (accueil de loisirs, crèches...) : une donnée relative à la santé d'une personne est une donnée sensible. En tant que données sensibles, les données relatives aux vaccinations des enfants ne pourront être traitées et collectées par l'association qu'avec le consentement des personnes. En pratique, soit une clause est insérée au contrat conclu avec les parents de l'enfant soit un formulaire spécifique de consentement devra être signé par les parents.

11. COMMENT FAIRE POUR ME METTRE EN CONFORMITÉ LORS DES INSCRIPTIONS AUX CENTRES DE LOISIRS ?

Voici deux exemples de formulaire qu'il est possible d'utiliser ou adapter pour son centre social

RGPD exemple de formulaire d'inscriptions enfants familles

RGPD exemple de formulaire pour la gestion des autorisations sur AIGA

12. COMMENT ME METTRE EN CONFORMITÉ POUR LE TRAITEMENT DES DONNÉES DE MES SALARIÉ.E.S ?

De très nombreuses données personnelles relatives aux employé.e.s sont nécessaires pour la gestion au sein de votre centre. Par exemple, vous avez besoin d'informations pour assurer la rémunération et les déclarations sociales obligatoires ; la gestion administrative du personnel (exemple : type de permis de conduire détenu ou coordonnées de personnes à prévenir en cas d'urgence) ; l'organisation du travail (exemple : photographie facultative de l'employé pour les annuaires internes et organigrammes)... Ne demandez à vos employés que les informations utiles pour accomplir leurs missions, et ne traitez pas de données dites « sensibles » (activité syndicale, opinions politiques, religion, origine ethnique, santé). Si vous devez en traiter, des obligations particulières sont applicables.

Au centre social, seules les personnes habilitées doivent avoir accès aux informations personnelles concernant les salarié.e.s. Les actions sur les données doivent être enregistrées. Il faut être en mesure de savoir qui se connecte, à quoi, quand et pour quoi faire sur les données.

Vos collaborateur.rice.s doivent être informé.e.s :

- chaque fois que vous leur demandez des informations (mise à jour des données administratives, demande de formation, formulaire d'entretien d'évaluation, etc.) ;
- De leur droit de consultation, modification et suppression des informations/données les concernant: les salarié.e.s peuvent vous demander une copie de toutes les données les concernant que vous détenez (bulletin de paie, état d'un compte épargne-temps, messages envoyés via le mail professionnel, y compris lorsqu'un.e employé.e n'est plus en poste ou est en litige avec vous.) Vous pouvez par exemple ajouter une annexe au contrat de travail de chaque salarié.e mentionnant son droit de consultation, modification et suppression de ses données personnelles.

NB : En ce qui concerne les recrutements, vous pouvez conserver les CVs des candidat.e.s jusqu'à un an maximum après leur réception.

13. QUELLE EST LA DURÉE MAXIMALE DE CONSERVATION DES DONNÉES ?

Les données relatives à gestion de la paie ou au contrôle des horaires des salarié.e.s peuvent être conservées pendant 5 ans.
Les données figurant dans un dossier médical doivent être conservées 10 ans à compter de la consolidation du dommage.
La CNIL recommande que les coordonnées d'un prospect qui ne répond à aucune sollicitation pendant 3 ans soient supprimées.
Pour le reste, les données doivent être conservées tant que vous en avez besoin mais doivent être supprimées dès lors que vous n'en avez plus l'utilité.

N'hésitez pas à nous faire remonter vos questions sur le RGPD ! (anouk.cohen@centres-sociaux.fr)

Pour aller plus loin

Profusion d'articles et guides ont été produits avec l'entrée en vigueur du RGPD. Au-delà d'outils qui s'appliquent à des entreprises de taille importante, quelques supports ont été produits à l'attention de structure de petite taille, ou d'associations. parmi ceux-ci, voici quelques ressources utiles :

LA RÉFÉRENCE, LA CNIL : Pour plus d'informations, vous pouvez consulter le site de la CNIL : www.cnil.fr.

Vous pouvez également visionner cette vidéo qui explique d'une manière simple et ludique le RGPD : « RGPD / GDPR : On répond à vos questions avec la CNIL » (sur youtube).

LE SYNDICAT EMPLOYEUR DES ACTEURS DU LIEN SOCIAL ET FAMILIAL : SNAECSO a organisé au printemps 2018 un webinaire afin d'informer sur les obligations liées au RGPD.
Celui-ci est accessible sur le site de la FCSF : http://www.centres-sociaux.fr/2018/05/17/rgpd-le-webinaire-du-snaesco/

Et si votre centre social est adhérent au Snaecso et que vous êtes employeur, vous pouvez joindre l'équipe de juristes qui pourra répondre à vos questions : https://www.snaecso.com/Nous-contacter

LE GUIDE DE SENSIBILISATION POUR LES TPE ET PME produit par BPI et la CNIL apportent nombre de conseils qui peuvent être suivis dans les centres sociaux : https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-guide-rgpd-tpe-pme.pdf

Fédération des centres sociaux et socioculturels de France [FCSF]
10 rue Montcalm - BP 379 F-75869 paris Cedex 18
www.centres-sociaux.fr - tél : 01.53.09.96.16

Fédération des centres socioculturels des Deux-Sèvres
46 Boulevard Edgar Quinet, 79200 Parthenay
www.csc79.org