GUIDE RGPD*

à l'attention des services sociaux membres de la FdSS FdSSB



* règlement général sur la protection des données

Comme vous le savez déjà, le **R**èglement **G**énéral sur la **P**rotection des **D**onnées (RGPD) est un règlement européen applicable à toutes les entreprises (y compris les petites ASBL) qui traitent des données personnelles des résidents de l'Union européenne depuis le 25 mai 2018.

Au printemps 2018, une séance d'information a été organisée par la FdSS-FdSSB. Etant donné la complexité de ce dossier, un **Comité de pilotage**[1] a été constitué avec des coordinateurs des services sociaux (CAP, CASG et CSS), la coordinatrice sectorielle de la FdSS-FdSSB et la collaboration de l'ASBL Ideji, dans le but de créer des outils standards de mise en conformité au RGPD, adaptés aux pratiques des services sociaux.

Le Comité de pilotage a rempli sa mission ; nous avons élaboré un **« kit standard » de mise en conformité spécifique** aux services sociaux membres de la FdSS (CASG, CAP, CSS, ILI, SASPP).

Le « kit standard » de mise en conformité comprend :
- un guide de mise en conformité
- un modèle de règlement interne (à annexer, une fois adapté à votre règlement d'ordre intérieur)
- des outils standards adaptés aux pratiques des services sociaux généralistes (9 annexes)
- un registre des activités de traitement de données

L'ensemble de ces outils a été pensé pour le secteur, vous devrez les adapter selon la réalité de votre service social.

Pour toute question, vous pouvez envoyer un mail à l'adresse : julie.kesteloot@fdss.be

1 Le comité de pilotage est composé, pour les coordinateurs des services sociaux : Alain Caufriez (CASG – Entr'Aide des Marolles) ; Marie-Christine Renson (CAP-SSQ1030), Arnaud De Temmerman (CAP – Les Amis d'Accompagner), Vincent Demulder (CASG – Service Social Juif), Sylvia Schlueppmann (CSS – CSSN), Gilles Hallez (CASG – Wo-lu-services), Marie-Noëlle De Decker (CASG – Pour les Familles) ; pour la FdSS-FdSSB : Julie Kesteloot ; pour IDEJI : Laure Morelli.

TABLE DES MATIÈRES

Préambule 5
Bon à savoir ! 6

Introduction 7
Principes généraux 7
Quelques définitions 8

Exercice des droits de la personne concernée 10
Consentement 10
Des usagers 10
Des travailleurs 10
Modification du consentement, retrait, effacement, accès 10

Constitution des registres 11

Délais de conservation 11

Règles relatives à la communication externe 11

Documents RGPD 12
Listes des documents obligatoires et modes de transmission 12
Documents et contrôle 14

PRÉAMBULE

Conformément à la réglementation européenne en matière de protection des données personnelles, les informations relatives à des personnes physiques ne peuvent être utilisées que de manière transparente et, le cas échéant, avec le consentement des personnes concernées.

En tant que travailleurs (salariés, volontaires, stagiaires), nous vous rappelons que vous êtes soumis à une obligation de confidentialité pour l'ensemble des données, notamment des informations personnelles, auxquelles vous avez accès dans le cadre de vos fonctions (qu'il s'agisse des données de bénéficiaires, volontaires, donateurs, salariés…).

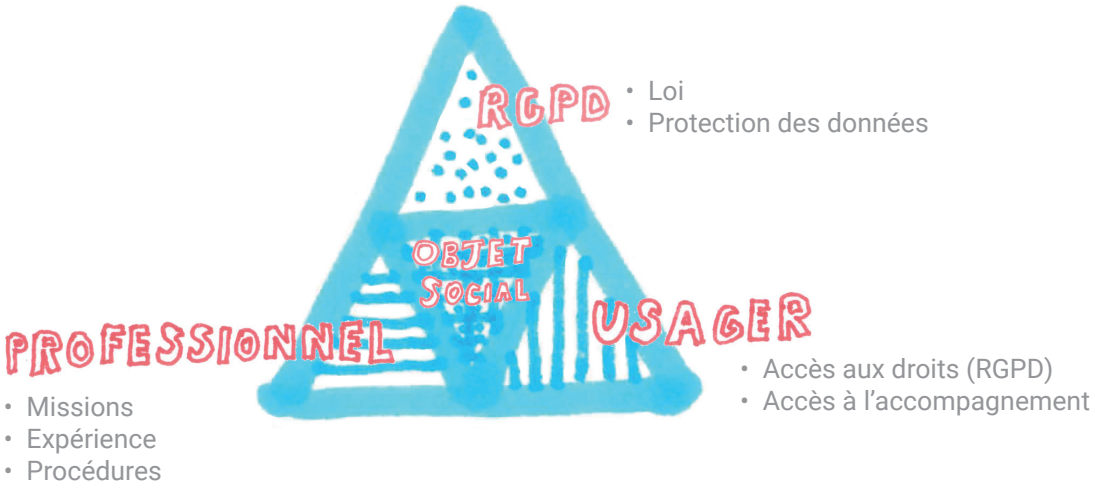
Tout usage ou réutilisation illicite de ces données constituerait une violation de la réglementation en matière de protection des données personnelles, et notamment du RGPD, et engagerait la responsabilité de l'association qui pourrait être sanctionnée par une amende administrative importante.

Par ailleurs, nous vous rappelons que chaque travailleur (salariés, volontaires, stagiaires) est soumis à un engagement contractuel de confidentialité à l'égard de son employeur et, qu'à ce titre, toute diffusion ou utilisation illicite d'informations est susceptible de sanctions disciplinaires.

Il est donc important que chacun d'entre vous soit vigilant quant à l'utilisation, la communication et la conservation des informations contenues dans nos bases de données et dans vos dossiers.

BON À SAVOIR !

L'application du RGPD sur le terrain impose une conception triangulaire tenant compte des préceptes dictés par la législation, de la réalité du travail d'accompagnement psycho-social et de la spécificité des usagers. Cette articulation peut être schématisée comme suit :



Elle signifie que, pour réaliser son objet social, l'association doit tenir compte de trois principes. Premièrement, elle est obligée de se conformer à la loi et donc au règlement européen qui, rappelons-le est inconditionnel quel que soit le siège social ou d'exploitation de l'entreprise sur le territoire européen, le type d'entreprise - en ce compris les ASBL -, le secteur - privé ou public - et l'activité menée - commerciale ou non marchande. Le RGPD ne s'intéresse pas à l'activité de la personne morale. Il ne donne accès, pour les personnes physiques, qu'à des droits concernant la protection de leurs données personnelles. Il ne se demande pas si l'application de ces droits pourrait venir perturber le travail social ni même empêcher la réalisation de certaines missions de base du service.

Deuxièmement, l'association se compose de travailleurs caractérisés par une expérience professionnelle qui leur permet de mettre en place des procédures spécifiques de prise en charge et d'accompagnement du public. Chaque professionnel est engagé pour remplir une partie des missions de l'ASBL. Ensemble, ils constituent une partie des outils dont dispose la structure pour réaliser son but.

Troisièmement, l'association accueille des usagers en demande d'un accompagnement psycho-médicosocial. Leur intérêt n'est évidemment pas uniquement porté sur leurs droits en matière de protection de leurs données personnelles. Ils sont motivés avant tout par la réalisation partielle ou complète du service pour lequel ils poussent la porte de l'institution.

Se placer uniquement du côté du texte de loi, c'est nier le fait que les travailleurs ont un professionnalisme et sont, pour certains d'entre eux, encadrés par un code de déontologie. C'est aussi nier la raison pour laquelle le public se déplace en association et l'objet même de sa demande, qui n'est pas prioritairement portée sur ses données personnelles mais bien sur un accompagnement, la participation à des activités, de l'information préventive… Une vision triangulaire de l'application du RGPD sur le terrain est donc essentielle pour ne pas passer à côté d'éléments essentiels qu'ils soient dans le chef des travailleurs ou des usagers.

INTRODUCTION

Le Règlement Général sur la Protection des Données (RGPD) est un règlement européen applicable à toutes les entreprises (y compris les petites ASBL) de l'Union européenne, depuis le 25 mai 2018. Le présent texte vise à mettre en application de manière concrète, au sein des services sociaux généralistes, ce règlement. C'est le conseil d'administration qui a la responsabilité juridique de la mise en conformité au RGPD, de votre association.

PRINCIPES GÉNÉRAUX

Le RGPD vise à renforcer le droit des personnes physiques à l'égard de l'utilisation (traitement) de leurs données personnelles. Il s'adresse à l'ensemble des acteurs des Etats membres et concerne toutes les personnes physiques, c'est-à-dire vos bénéficiaires et vos travailleurs.

La règle générale est qu'il est interdit à toute institution de posséder et d'utiliser des données à caractère personnel, **sauf** lorsque l'association peut justifier d'une raison valable à ces traitements, appelée « fondement légal ». Il existe 6 fondements légaux. Ils ne sont pas cumulatifs (= pour chaque traitement, un seul doit s'appliquer) :

- La personne a donné son **consentement** pour l'utilisation de ses données dans un but précis (pas d'autorisation générale). Exemple : le bénéficiaire a donné son accord pour être contacté par téléphone ;

- L'entreprise a une **obligation légale** de conserver ces données. Exemple : un décret/une ordonnance vous oblige à justifier vos subsides en fournissant le cadre du personnel à votre pouvoir subsidiant ;

- Ces données sont nécessaires à l'exécution d'un **contrat**. Exemple : l'usager s'adresse à votre service pour être accompagné (tout ce qui relève de sa demande d'accompagnement fait partie du contrat) ;

- Ces données sont nécessaires à la **sauvegarde des intérêts vitaux** de la personne concernée. Exemple : vous devez prévenir la famille, la police… si vous pensez que la personne est en danger ;

- L'entreprise effectue une **mission d'intérêt public** : ce n'est pas votre cas ! (la police, l'armée, les pompiers, les ambulanciers, les SPF et le service Population des communes ont une mission d'intérêt public) ;

- L'association a un **intérêt légitime** à utiliser ces données et cela n'est pas (trop) préjudiciable pour la personne par rapport à sa vie privée. A utiliser avec beaucoup de précaution :
  - Il est interdit pour le traitement de données des bénéficiaires ;
  - Il est autorisé pour le traitement des données des travailleurs, si cela ne le met pas en danger et si cela ne nuit pas à sa réputation ;
  - Il est autorisé pour le traitement des données des donateurs.

En tant que services sociaux généralistes, nous sommes fortement concernés parce que nous « traitons » de nombreuses données personnelles essentiellement de 2 types : les données sociales et administratives de nos usagers, et les données administratives des collègues.
Il s'agit donc de mettre en œuvre, progressivement, un processus et un ensemble de règles à respecter qui permettent d'augmenter le niveau de **droits** et de **sécurité**, tout en sachant que la sécurité totale n'existe pas mais qu'il y a lieu d'essayer de l'améliorer constamment. C'est ce que le RGPD appelle : la **mise en conformité**.

Attention : Le RGPD a été mis en place suite aux développements de l'informatique et des flux de données qu'elle génère, mais il concerne AUSSI les autres supports tels que le papier.

Un des principes importants du RGPD est que nous ne pouvons « traiter » des données à caractère personnel que dans les limites de ce qui est nécessaire pour exécuter notre mission. C'est le principe de « limitation des données ». Toute donnée dont vous n'avez pas besoin et qui ne fait pas partie d'une obligation légale doit être détruite. Comme il est plus simple de limiter que de détruire, nous vous conseillons de revoir vos « fiches d'inscription » et d'en éliminer tout ce qui ne doit pas s'y trouver de manière standardisée. => ne demandez au bénéficiaire que ce qui est effectivement nécessaire à sa prise en charge (et surtout pas ce qui pourrait éventuellement être utile).

QUELQUES DÉFINITIONS

Le RGPD utilise un langage spécifique qu'il est utile de préciser :

- Donnée à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable.
  - Une personne physique est identifiée par son nom, numéro de registre national ou son numéro d'affiliation à la mutuelle ;
  - Une personne physique est identifiable par un ensemble d'éléments qui permettent de retrouver précisément de qui il s'agit. (Remarque : en équipe, il est normal que vous sachiez de qui vous parlez ! La sécurité est là pour protéger la personne contre les intrusions externes.)

Concrètement, les données que nous utilisons habituellement dans les SS sont[2] :

• Concernant les travailleurs :
- Nom, prénom
- Date de naissance,
- NN
- Adresse
- Téléphone
- Email
- Photos
- Données salariales : ancienneté, barèmes, diplôme, compte bancaire, certificats maladie

• Concernant les usagers
- Nom, prénom
- Date naissance
- Nationalité
- Adresse
- Téléphone
- Situation socio-économique
- Sexe
- Type de ménage
- Identité membres du ménage
- Type de logement
- Type de domicile
- Situation administrative étranger
- Données sociales (problématiques)

Certaines données sont réputées sensibles, d'autres non sensibles.
C'est l'analyse des risques, liée au registre de traitements, qui le détermine.

2 Cette liste est donnée à titre indicatif et peut être adaptées à votre réalité).

- Donnée sensible : toute information devant donner lieu à un niveau de sécurité et de justification plus élevé et relevant de l'origine raciale ou ethnique, de conviction religieuse ou philosophique, de l'appartenance syndicale, de la génétique, de la biométrie, de la santé, de la vie sexuelle ou de l'orientation sexuelle.

- Traitement des données : à entendre dans un sens très large : enregistrement, stockage et utilisation de données (=> le traitement n'est donc pas uniquement une action. Ne rien faire d'une donnée archivée, c'est déjà la traiter).

- Responsable de traitement : c'est l'ASBL, et donc son conseil d'administration, qui est juridiquement responsable. Il confie sa mise en œuvre à un **référent RGPD** (une ou plusieurs personnes désignées par le conseil d'administration pour suivre la mise en conformité du service au RGPD).

- Sous-traitant : les services que votre association utilise pour remplir son objet social et que la loi lui permettrait (sens et finances mis à part) de développer en interne = secrétariat social, informaticien externe, comptable externe, service de traduction ou d'interprétariat…



EXERCICE DES DROITS DE LA PERSONNE CONCERNÉE

CONSENTEMENT

CONSENTEMENT DES USAGERS

Le consentement de l'usager est nécessaire quand aucun autre fondement légal de traitement ne s'applique[3]. Il concerne, par exemple, l'envoi d'information à son domicile, l'organisation de réunion de concertation, le contact d'un partenaire de réseau pour un complément d'accompagnement…

Si le consentement est nécessaire il y a lieu de faire signer, en 2 exemplaires, le formulaire ad hoc (voir annexe) : Un des formulaires est remis au patient, l'autre est conservé à l'association.

Il ne suffit pas de demander le consentement d'un bénéficiaire, encore faut-il respecter son choix. Veillez à conserver les formulaires de consentement dans un lieu (informatisé ou non) facilement accessible pour vos travailleurs.

CONSENTEMENT DES TRAVAILLEURS

L'utilisation de certaines données du personnel non indispensable à l'exécution du contrat de travail (obligation légale), nécessitent le consentement de la personne : GSM personnel, photo, e-mail personnel, e-mail professionnel nominatif, carte de visite nominative, liste du personnel sur le site internet de l'association…

Dans ce cas il est nécessaire de faire signer le formulaire de consentement par le travailleur. (voir annexe)

MODIFICATION DU CONSENTEMENT, RETRAIT, EFFACEMENT, ACCÈS

Toute personne physique (bénéficiaire ou travailleur) est en droit de demander la rectification, l'effacement, l'accès, l'inventaire de ses données. Pour garantir la sécurité, la personne doit prouver son identité en présentant sa carte d'identité. L'association est dans l'obligation de s'exécuter, lorsque la demande est légitime et non régie par une règlementation/loi. Dans tous les cas – légitimité ou non –, l'association doit répondre à la demande, par écrit, afin de confirmer à la personne physique, l'exécution de ses droits ou la limite de ceux-ci en regard de la législation.

Toute demande d'effacement de données doit être exécutée (si légitime) dans les trente jours suivant la demande. Tout retrait de consentement est lui actif immédiatement. Néanmoins, il n'est en aucun cas rétroactif.

Afin d'informer correctement les usagers sur leurs droits, une affiche (voir annexe) est apposée de manière bien visible dans la salle d'attente.

3 Pour rappel : quand l'usager s'adresse à votre service pour être accompagné, le consentement n'est pas nécessaire, tout ce qui relève de sa demande d'accompagnement fait partie du « contrat ».

CONSTITUTION DES REGISTRES

Le service social constitue 2 registres distincts :
- Le registre des activités de traitement des données ou R.A.T. (voir annexe)
- Le registre des incidents

En ce qui concerne les consentements, le service social doit s'organiser pour les retrouver facilement (sous forme de registre, dans les dossiers individuels, feuille Excel, farde, etc.).

DÉLAIS DE CONSERVATION

Au moins une fois par an, le service social procède à l'effacement systématique des données qui ont atteint leur date limite de conservation Les délais de conservation maximale, pour les données les plus utilisées en services sociaux sont :
- Données administratives des usagers : 7 ans
- Données des travailleurs:
  - CV, contrats, fiches de paye : 5 ans ;
  - relevés annuels individuels, déclarations ONSS et précompte professionnel : 10 ans
- Données comptables (factures, bons de commande, ...) : 7 ans
- Candidatures à l'emploi : 6 mois à 1 an.

Au niveau papier : les documents contenant des données personnelles doivent impérativement être détruits par déchiqueteuse. Si une personne le demande et si sa demande est légitime, le service social procèdera à l'effacement des données endéans le mois de la demande.

RÈGLES RELATIVES À LA COMMUNICATION EXTERNE

Le service social s'engage à informer les personnes, lors de sa communication externe sur internet, sur leurs droits en matière de RGPD.
Pour ce faire, il veille à mettre les messages ad hoc sur ses outils de communication.

DOCUMENTS RGPD

LISTES DES DOCUMENTS OBLIGATOIRES ET MODES DE TRANSMISSION

Tous les documents obligatoires ont été adaptés (par le Comité de pilotage RGPD) et sont repris en annexe de ce règlement interne.

	Nom du document	Description	À qui il s'adresse	Modalités de diffusion
1	Politique de confidentialité	Il s'agit d'un document global reprenant de manière synthétique la raison de la collecte des données, leur(s) destination(s), la sécurité que vous mettez en place pour les protéger et leur conservation.	Tout public	Doit être placée sur votre site internet + disponible à l'accueil
2	Politique de sécurité	Il s'agit d'un document reprenant très précisément les mesures de sécurité mises en place par le service social. Il n'est en aucun cas public (puisqu'il parle de votre système de sécurité). A l'extérieur du service, seuls les sous-traitants doivent le recevoir puisque le RGPD met en place un système de coresponsabilité.	Uniquement les travailleurs et les sous-traitants (comptable externe, informaticien externe, secrétariat social…)	Pour les travailleurs : accessible sur le serveur (ou si vous la faite signer alors chaque document signé va dans le dossier RH du travailleur) Pour les sous-traitants : envoyée au sous-traitant (le sous-traitant signe votre politique des sécurité - vous signez la politique de sécurité du sous-traitant = échange de bons procédés)
3	Droits des usagers et des travailleurs (texte identique)	Il s'agit d'un document standard reprenant les droits des usagers et des travailleurs dans le cadre du traitement, de l'accès, de la modification et de la transmission de leurs données.	Usagers et travailleurs	Affichés en salle d'attente et en salle d'équipe

	Nom du document	Description	À qui il s'adresse	Modalités de diffusion
4	Formulaire de consentement des travailleurs	Il s'agit d'un document reprenant tous les points pour lesquels le service social est susceptible d'avoir besoin du consentement spécifique du travailleur pour pouvoir effectuer le traitement. Tous les travailleurs doivent impérativement le compléter.	Travailleurs	Dans le dossier RH de chaque travailleur
5	Formulaire de consentement des usagers	Il s'agit d'un document reprenant tous les points pour lesquels le service social est susceptible d'avoir besoin du consentement spécifique du bénéficiaire pour pouvoir effectuer le traitement. Tous les bénéficiaires doivent impérativement le compléter.	Usagers	Dans le dossier des bénéficiaires ou dans un dossier à part regroupant tous les consentements (informatisé ou papier)
6	Engagement de confidentialité des personnes ayant vocation de traiter des données personnelles	Il s'agit d'un formulaire officiel transmis par l'Autorité de protection des Données (organe de contrôle en Belgique). Chaque travailleur (au sens large : salarié, indépendant, étudiant, volontaire) ayant accès à des données personnelles de bénéficiaires et/ou de travailleurs doit impérativement signer ce document.	Travailleurs	Impérativement signé par chaque travailleur et placé dans son dossier RH
7	Message internet	Il s'agit de messages destinés à informer les personnes, lors de sa communication externe sur internet, sur leurs droits en matière de RGPD.	Tout public	Site internet, newsletter, formulaires d'inscription en ligne,...
8	Clause sous-traitance (8a) et lettre type (8b) pour échange politique de sécurité	Il est probable, si vous utilisez les services d'un sous-traitant (secrétariat social, comptable externe, informaticien externe...) que vous ayez déjà un contrat de sous-traitance. Néanmoins, certaines structures n'ayant jamais pensé faire ce genre de documents, l'Autorité de protection des Données en a mis en place pour vous aider. Nous l'avons joint aux annexes de ce kit RGPD.	Sous-traitants	Annexe aux contrats de sous-traitance

	Nom du document	Description	À qui il s'adresse	Modalités de diffusion
9	Protection des données de candidatures (offres d'emploi)	Message type de réponse à adresser aux personnes qui ont adressé leur candidature à une offre d'emploi et dont vous souhaitez conserver les candidatures non retenues dans une base de recrutement.	Personnes qui ont adressé leur candidature à une offre d'emploi	Annexe aux candidatures conservées dans une base de recrutement
10	Registre d'Activités de Traitement (RAT)	Ce registre, sous forme de tableau Excel, est la première chose qui sera demandée en cas d'inspection. Il doit absolument être complété et suivre la vie de votre association. Cela signifie que, même si la FdSS vous en fourni un exemplaire, vous devez le lire attentivement et y indiquer ce qui concerne votre service social. Exemple : si actuellement vous n'avez pas de volontaire, vous devez supprimer les références aux volontaires. Vous devrez rajouter ces références le jour où vous aurez des volontaires.		Tableau Excel interne reprenant tous les traitements possibles dans votre association
11	Cahier des incidents	Ce cahier reprend la liste de tous les risques (perte de clé ou de données, perte de mot de passe…) et de toutes les intrusions (vol, piratage informatique…) qui mettent à mal la sécurité des données des travailleurs ou des bénéficiaires.		Cahier interne (version électronique ou papier) reprenant tous les risques à la sécurité (perte de clé, infraction dans le bâtiment, perte de dossiers usagers…)

DOCUMENTS ET CONTRÔLE

En cas de contrôle, l'inspecteur vous demandera :

- Un exemplaire vierge de chaque document (politique de sécurité, politique de confidentialité, droits des usagers et travailleurs, formulaires de consentement, engagement de confidentialité) ;
- Votre Registre d'Activités de Traitement (RAT) ;
- Votre cahier des incidents ;
- Votre politique de sécurité signée par les sous-traitants ;

La politique de sécurité de vos sous-traitants signé par vous.

FdSS
FdSSB



- Juillet 2019 -
ER : Céline Nieuwenhuys, Fédération des Services Sociaux,
rue Gheude 49 à 1070 Bruxelles