Le RGPD et les CPAS : menace ou opportunité ?

E. Dheygere, juriste (avril 2018)

Depuis plusieurs mois déjà, le Règlement Général sur la Protection des Données (RGPD) adopté par l'Union Européenne est devenu l'une des préoccupations majeures de bons nombres d'organisations privées ou publiques. Ce règlement, adopté le 27 avril 2016 et qui entrera en vigueur le 25 mai 2018[1], fait l'objet de nombreuses (in)formations qui reflètent la complexité du sujet. Toutefois, les spécialistes s'accordent sur un point : il n'existe pas une solution unique permettant d'être conforme au RGPD. Cet article n'aura donc pas pour vocation de fournir une proposition exclusive, mais bien des pistes de solutions afin d'atteindre l'objectif visé : le respect de la vie privée.

Pour pouvoir déterminer les processus à mettre en œuvre pour atteindre l'objectif « RGPD », il est primordial d'en comprendre la philosophie. Il est donc important de rappeler que le RGPD n'est pas une nouveauté en soi. En effet, seul 20 % du règlement peut être considéré comme tel par rapport à la loi « vie privée » en vigueur en Belgique depuis 1992[2]. Ainsi, le RGPD maintient les fondamentaux de la loi « vie privée » (donnée à caractère personnel, traitement, responsable du traitement, légitimité du traitement…)[3]. La vocation de ce nouveau règlement, outre d'harmoniser les législations nationales, est :

- de permettre une protection des données adaptée aux nouvelles réalités numériques ;
- d'octroyer aux personnes concernées un meilleur contrôle de leurs données ;
- de mettre les organismes de traitement en situation de responsabilité.

Il ne s'agit donc pas de mettre en place, à la hâte, certains processus pour se conformer aux obligations du règlement, mais bien de réfléchir à la manière d'intégrer cette philosophie de protection optimale des données dès l'origine et la conception d'un service. En d'autres termes, pour réussir à implémenter le RGPD, il ne suffit pas d'imbriquer des procédures complexes à une organisation qui n'en comprend pas le but. Il faut, à l'inverse, commencer par transformer l'organisation interne afin d'ancrer cette réflexion de manière transversale… Un challenge !

En termes de cadre législatif, le RGPD remplace la loi « vie privée ». Par ailleurs, une loi-cadre, actuellement en cours d'analyse par la Conseil d'Etat, et dont l'entrée en vigueur est prévue prochainement, viendra compléter le RGPD. Les lois sectorielles (telles que la loi « bcss » de 1990[4], la loi « registre national » de 1983[5]) sont, elles, maintenues et toujours d'application.

Le CPAS, soumis au RGPD ?

A travers sa mission d'aide sociale, le CPAS est amené à traiter de manière continue des données à caractère personnel (autrement dit, les données qui identifient ou rendent identifiables une personne physique).

Prenons l'exemple du service de médiation de dettes d'un CPAS. Lors du premier rendez-vous avec le citoyen, l'employé sera amené à collecter une série d'informations personnelles tels que le nom, le prénom, le numéro de téléphone, l'adresse, le numéro de registre national, la composition de ménage,

[1] Règlement (UE) 2016/679 du 27 avril 2016
[2] Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel
[3] Voir les définitions : Règlement (UE), 2016/679 du 27 avril 2016, art. 4
[4] Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale
[5] Loi du 8 août 1983 organisant un registre national des personnes physiques

les ressources, les dettes… Un dossier est créé en format papier ou informatique, dans lequel figure l'ensemble des informations recueillies. Ce dernier est classé et rangé avec d'autres dossiers similaires. La collecte des données, la création de ce dossier et sa conservation sont considérées comme un traitement de données à caractère personnel au sens du RGPD. Le CPAS, en sa qualité de personne morale de droit publique, est ainsi soumis au RGPD en tant que responsable du traitement et doit donc se conformer à certaines obligations.

Quelles sont les obligations à charge du CPAS ?

La philosophie que doit suivre le CPAS pourrait se résumer comme suit : traiter les données des autres, comme on voudrait que nos données soient traitées. Ainsi, le RGPD met un point d'honneur à imposer les mesures suivantes[6] :

- des traitements licites ;
- une loyauté et transparence d'informations ;
- une détermination des finalités du traitement et de ses limites ;
- un traitement limité aux données adéquates, pertinentes et nécessaires ;
- une utilisation de données exactes ;
- une conservation des données limitée ;
- une sécurité importante des traitements ;
- une responsabilisation du responsable de traitement.

Le RGPD définit également les droits des personnes concernées[7]. Ainsi, le responsable du traitement des données doit pouvoir répondre de manière compréhensible, dans les meilleurs délais et sans exiger le moindre paiement, aux droits suivants :

- droit à l'information ;
- droit d'accès ;
- droit de rectification ;
- droit à l'effacement « droit à l'oubli » ;
- droit à la limitation du traitement ;
- droit à la portabilité des données (concerne peu les CPAS) ;
- droit d'opposition ;
- droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé (concerne peu les CPAS actuellement).

Le CPAS qui répond à ces différents droits et obligations pourra justifier sans crainte les traitements de données à caractère personnel qu'il réalise. Reprenons notre exemple afin de comprendre le raisonnement à tenir, afin de s'assurer du respect de ces droits et obligations.

Le CPAS décide d'octroyer une aide sociale sous la forme d'une médiation de dettes. Des données vont être collectées par le travailleur social du CPAS afin d'assurer au mieux sa mission. Pour que ce traitement soit **licite**, il faut justifier son fondement. Le RGPD prévoit 6 fondements différents :

- le consentement ;
- le contrat ;
- l'obligation légale ;
- l'intérêt vital ;
- l'exécution d'une mission d'intérêt public ;
- l'intérêt légitime.

[6] Règlement (UE), 2016/679 du 27 avril 2016, art. 5.
[7] Règlement (UE), 2016/679 du 27 avril 2016, Chapitre III « Droits de la personne concernée », art. 12 et s.

En ce qui concerne les CPAS, les données collectées l'ont été en raison d'une **obligation légale** (mission d'aide sociale prévue par la loi du 8 juillet 1976, article 60 §1er ; Circulaire unique du 13 octobre 2017 relative à la médiation de dettes qui prévoit la fiche de suivi standardisé). En général, le traitement des données à caractère personnel réalisé par un CPAS est souvent justifié par une base légale (à déterminer précisément !) ou par la nécessité d'exécuter une **mission d'intérêt public**. A défaut, il faudra veiller à obtenir le **consentement** libre, spécifique, éclairé et non présumé de la personne concernée.

Dans le cadre de la collecte des données, le CPAS doit également faire preuve de **loyauté et de transparence,** ce qui se traduit par une obligation d'information (// droit d'information) claire et concise des raisons de la collecte et de la manière dont les données seront utilisées. On en vient ainsi à définir **les finalités** du traitement et l'interdiction d'utiliser les informations collectées à d'autres fins incompatibles. Ainsi, par exemple, les données collectées pour répondre à une demande de médiation de dettes ne pourront être légalement transférées à une société marketing afin d'adresser des publicités. Par contre, il est très probable que le transfert d'informations pour l'obtention automatique de droits dérivés pour les personnes en règlement collectif de dettes (tel que le statut de client protégé), sera prévu dans les finalités du traitement ou jugé compatible.

Enfin, les données collectées doivent être **adéquates, pertinentes et nécessaires**. Ainsi, le CPAS ne peut disposer d'informations relatives à l'origine ethnique ou encore à l'orientation politique qui sont, dans notre exemple, sans influence sur la demande de médiation de dettes. Les données doivent également être **exactes** (// droit de rectification) et leur **conservation limitée**.

Au-delà des obligations, le RGPD a également clarifié les droits des personnes concernées. On y retrouve, par exemple, le « droit à l'oubli » ou le « droit à la limitation du traitement ». Le premier leur permet d'exiger l'effacement de données qui ne seraient plus nécessaires, qui auraient été recueillies de manière illicite ou encore pour lesquelles leur consentement aurait été retiré. Le deuxième leur permet de demander au responsable de limiter le traitement des données dans différents cas de figure (par exemple, une personne peut demander au CPAS que ses données ne soient pas effacées, mais ne soient plus traitées sans son consentement). Il est également possible, pour les personnes concernées, de s'opposer au traitement de leurs données (par exemple, lorsque celles-ci sont utilisées à des fins de prospection). Dans ce cas, le CPAS doit démontrer qu'il est en droit de traiter malgré tout ces données.

À tout moment, une personne a le droit de demander d'**avoir accès** à toutes les informations que le CPAS détient sur elle, et de connaitre la ou les raisons de cette détention/utilisation de données. En d'autres termes, il faudrait imaginer un système (par exemple, un site internet) répertoriant, par personne, les catégories de données, le responsable de traitement, la finalité… et auquel les personnes concernées pourraient avoir accès.

Le CPAS doit également assurer la **sécurité** des traitements et du système informatique, que ce soit en interne ou en externe. Ainsi, des accès internes devront être déterminés en fonction des gestionnaires de dossiers et de la nécessité. Le système informatique devra également être sécurisé dans la meilleure mesure du possible afin d'éviter toute fuite, piratage…

Quels outils mettre en œuvre ?

Le RGPD place le responsable du traitement en situation de responsabilisation. Cela signifie que le CPAS doit être capable de démontrer lui-même sa conformité et son respect des obligations du RGPD. C'est dans cet objectif que plusieurs mesures ont été instaurées par le règlement à destination des responsables du traitement.

Premièrement, le CPAS devra désigner un **délégué à la protection des données**[8], appelé communément DPD. Il s'agit d'une obligation pour tous les organismes publics. Le rôle du DPD est

[8] Règlement (UE), 2016/679 du 27 avril 2016, art. 37 et s.

de veiller à ce que le CPAS traite les données à caractère personnel dans le respect du RGPD. Il servira également d'intermédiaire avec l'Autorité de protection des données (APD), l'organisme de contrôle qui n'est autre que l'actuelle Commission de la protection de la vie privée (CPVP). Cette personne doit donc revêtir à la fois des qualités juridiques et techniques afin d'exercer sa mission. Concernant le rôle du conseiller en sécurité au sein des CPAS, une interrogation persiste sur la possibilité d'unifier les deux fonctions. De plus, rien ne s'oppose à ce qu'un DPD unique soit désigné pour plusieurs CPAS ou encore qu'une structure en place, telle qu'une Association chapitre XII, élargisse son objet social afin d'intégrer cette nouvelle compétence.

Deuxièmement, le CPAS devra tenir un **registre de traitement**[9]. Il s'agit également d'une obligation pour tous les organismes publics. Ce registre remplace, en quelque sorte, la déclaration anciennement introduite à la CPVP. Ce registre constitue un inventaire des traitements de données à caractère personnel réalisés par le CPAS. La catégorie des données, leurs origines, les personnes y ayant accès, les finalités de traitement, les éventuels sous-traitants ou encore la durée de conservation doivent être définis clairement dans ce registre. Actuellement, la CPVP a élaboré un modèle de registre en format Excel, disponible sur son site internet[10]. Un modèle adapté aux CPAS est également en ligne sur le site du SPP Intégration sociale[11].

Troisièmement, le CPAS devra réaliser une **analyse de l'impact**[12] d'un traitement de données sur la vie privée des personnes concernées. Cette analyse est obligatoire lorsque le traitement de données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. En fonction des résultats de cette analyse, le CPAS ou plus particulièrement son DPD devra déterminer les mesures appropriées à prendre afin de demeurer conforme au RGPD. Pour ce faire, une recommandation vient d'être publiée par le Groupe 29[13], apportant plus de détails quant à cette démarche et un outil a été mis en place par la CNIL[14] (équivalent français de la CPVP) permettant la réalisation d'une telle analyse.

Quel rôle pour la Commission de la protection de la vie privée ?

La Commission de la protection de la vie privée (CPVP) deviendra, avec l'entrée en vigueur du RGPD, le nouvel organisme de contrôle appelé Autorité de protection des données (APD). De manière générale, l'APD aura pour mission de contrôler le respect du RGPD au sein des différents organismes qui y sont soumis. A côté de ce pouvoir de contrôle, l'Autorité aura également la possibilité de sanctionner administrativement les responsables de traitement en imposant un rappel à l'ordre, une limitation ou interdiction de traitement ou encore une amende administrative dissuasive plafonnée à 20 millions d'euros.

Cependant, il convient d'indiquer que, dans le projet actuel de loi-cadre accompagnant le RGPD, il serait question de ne pas rendre les amendes administratives applicables aux pouvoirs publics, et donc aux CPAS. Ceci n'empêche pas que d'autres sanctions pourraient intervenir par l'intermédiaire du juge qui serait saisi d'une plainte ou d'une action en responsabilité.

Quelles leçons tirer pour les CPAS ?

En conclusion, bien que le RGPD soit un garant indispensable du droit au respect de la vie privée, l'application de ce nouveau règlement constitue avant tout un véritable défi pour la plupart des organismes qui y sont soumis.

[9] Règlement (UE), 2016/679 du 27 avril 2016, art. 30.
[10] Modèle de registre proposé par la CPVP
[11] Modèle de registre adapté aux CPAS proposé par le SPP IS
[12] Règlement (UE), 2016/679 du 27 avril 2016, art. 35.
[13] Recommandation du Groupe 29
[14] Outil proposé par la CNIL

De manière plutôt positive, nous constatons que le traitement des données à caractère personnel réalisé par un CPAS est bien souvent justifié par une base légale ou par la nécessité d'exécuter une mission d'intérêt public**.** Ainsi, les CPAS ne doivent que peu s'inquiéter de devoir justifier l'utilisation de données à caractère personnel auprès de l'organisme de contrôle. En outre, les amendes administratives ne devraient pas s'appliquer en cas de défaut de conformité.

Toutefois, cela ne dispense pas les CPAS de mettre en œuvre les différents processus de conformité (DPD, registre, analyse d'impact). Ainsi, le challenge pour ces organismes publics se traduit principalement par un accroissement important des tâches administratives et d'encodage, par une modification de l'architecture organisationnelle des structures et par la mise en place de nouveaux processus et emplois spécifiques à la règlementation.