Délégué à la protection des
ses responsabilités et celles

Le 28 février dernier, la Fédération des CPAS organisait le premier événement de la « Plateforme DPD » qu'elle a souhaité mettre en place, afin de favoriser le partage d'expériences et de pratiques entre les acteurs de terrain concernés par la mise en œuvre du RGPD en CPAS.
Ce premier événement avait, volontairement, un programme panaché afin d'aborder une diversité de questions et de perspectives. Une des interventions, celle de Loïck Gérard[1], avait pour objectif de clarifier les risques et responsabilités du CPAS en cas de non-conformité au RGPD. Un focus particulier a été fait, par lui et par le second orateur Gilles Kempgens[2], sur la question de la désignation du délégué à la protection des données par le CPAS.
Nous revenons, dans cet article, sur les principaux enjeux et sur les modalités concrètes de cette désignation.

JUDITH DUCHÊNE
Conseillère

Suppression de la fonction du « conseiller en sécurité »

Du fait de leur connexion à la BCSS, les CPAS sont soumis aux dispositions prévues par l'Arrêté royal (A.R.) du 12.08.1993 relatif à la sécurité de l'information dans les institutions de sécurité sociale[3]. Ce dernier a été modifié par l'AR du 21.12.2018[4] (MB du 16.01.2019), ce qui a eu pour incidence de remplacer la fonction de « conseiller en sécurité de l'information » par celle de « délégué à la protection des données » (DPD).

Il convient de noter que le « conseiller en sécurité » ne devient pas automatiquement le DPD.

Concrètement, deux cas de figure peuvent se présenter :

- soit l'ancien « conseiller en sécurité » cesse d'exercer cette fonction au sein du CPAS et continue, tout simplement, à exercer ses autres fonctions. Dans ce cas, le Conseil de l'action sociale doit désigner une autre personne en tant que DPD, dans le respect des exigences du RGPD ;
- soit, après un examen d'opportunité, compte tenu des exigences du RGPD et moyennant son accord, l'ancien « conseiller en sécurité » sollicite sa désignation par le Conseil de l'action sociale comme DPD, en remplacement de ses anciennes fonctions.

Désignation d'un DPD

L'article 37 du RGPD rend obligatoire, pour toute autorité publique[5], la désignation d'un DPD. Le CPAS étant une autorité publique, il doit obligatoirement désigner un DPD.

Pour cette désignation, le CPAS doit s'assurer que le DPD envisagé dispose :

- des qualités professionnelles requises, en ce compris des connaissances spécialisées du droit et pratiques en matière de protection des données ;
- de sa capacité à exercer les missions qui lui sont attribuées par le Règlement, à savoir notamment[6] :
  - informer et conseiller le CPAS ou le sous-traitant, ainsi que les employés qui procèdent au traitement, sur les obligations qui leur incombent en vertu du règlement et d'autres dispositions du droit en matière de protection des données ;
  - contrôler le respect du RGPD, d'autres dispositions du droit en matière de protection des données et des règles internes du CPAS ou du sous-traitant en matière de protection des données (répartition des responsabilités, sensibilisation et formation du personnel participant aux opérations de traitement, audits s'y rapportant) ;
  - dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci ;
  - coopérer avec l'autorité de contrôle ;
  - faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement.

Absence de conflit d'intérêt

Par ailleurs, dans le cadre de la désignation du DPD, **le CPAS doit veiller à ce que celui-ci ne soit pas dans une situation de conflit d'intérêt** ; qu'il n'exerce pas une fonction au sein du CPAS qui l'amène à être juge et partie. Il convient d'éviter les cas où une personne prend des décisions relatives à des traitements de données ou aux mesures de sécurité qui encadrent ces traitements et que, par la suite, cette même personne rende un avis sur les règles et les processus internes au CPAS relatifs au traitement de données.

Le DPD ne peut donc **pas** être : un grade légal, un directeur du personnel, un responsable de service informatique.

Indépendance (droit de « déranger ») et soutien

Le DPD doit également disposer d'une indépendance : il ne peut recevoir aucune instruction du responsable du traitement (CPAS). L'idée est de lui préserver un « droit de déranger » : le droit d'aller mettre son nez dans les traitements de données à caractère personnel, dans les pratiques de protection de ces traitements, le droit d'aller poser des constats qui ne vont pas forcément arranger l'institution ou ses décideurs.

---

1 L. Gérard, Assistant, CRIDS, Faculté de Droit, UNamur.
2 G. Kempgens, DPD du SPP IS.
3 M.B., 21.08.1993.
4 A.R. du 21.12.2018 mod. l'AR du 12.08.1993 rel. à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale et l'A.R. du 20.09.2012 organisant la sécurité de l'information au sein de la plate-forme eHealth et fixant les missions et les compétences du médecin sous la surveillance et la responsabilité duquel s'effectue le traitement de données à caractère personnel rel. à la santé par la plate-forme eHealth, M.B. 16.01.2019.
5 L'art. 5 de la L. du 30.07.2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (M.B. 05.09.2018) donne une définition de ce qui doit être entendu par « autorité publique ».
6 Les missions du DPD sont précisées à l'art. 39 du RGPD.

données (DPD) : du CPAS !

« Le DPD doit disposer d'une indépendance. L'idée est de lui préserver un 'droit de déranger' »

Cette indépendance veut également dire que le délégué **doit recevoir le soutien du CPAS**.

Le DPD doit avoir une implication dans les décisions qui touchent les traitements de données **à un moment où son implication peut être encore utile** ; pas au moment où tout est fait et où il ne pourrait rendre qu'un avis purement formel.

Ce soutien doit également se matérialiser en **un temps et des moyens suffisants pour effectuer ses missions** (avoir accès aux données, droit de suivre des formations…).

Le DPD doit pouvoir être en contact direct avec le plus haut niveau de hiérarchie du CPAS, afin d'éviter que son avis soit reformulé ou retravaillé par d'autres membres de l'administration, pour le rendre plus lisse ou le vider de sa substance avant d'arriver au niveau de la direction.

Notification de l'identité du DPD

L'identité du DPD doit être transmise à plusieurs acteurs :

- à l'Autorité de protection des données (APD)[7] ;
- à la Banque Carrefour de la Sécurité sociale[8] ;
- au SPP IS[9].

En cas de non-conformité au RGPD, qui peut être à la base d'une sanction ?

L'article 83 du RGPD donne une série d'exemples de non-conformités qui peuvent être sanctionnées : sécurité insuffisante, choix d'un sous-traitant manifestement peu sérieux, absence de contrat de sous-traitance, absence ou insuffisance du registre des activités du traitement, absence ou insuffisance d'analyse(s) d'impact, absence de notification d'une violation de données, absence de DPD/atteinte au statut du DPD.

Plusieurs acteurs peuvent être à la base d'une procédure de sanction.

La personne concernée, celle dont le CPAS traite les données, dispose de trois voies d'action. Si elle estime être lésée, elle peut introduire un recours auprès d'un juge civil, d'un juge pénal ou de l'APD.

La personne concernée peut être représentée par une asbl active dans le domaine de la protection des données.

« Parmi les infractions de non-conformité au RGPD qui peuvent être sanctionnées, on peut citer l'absence de désignation d'un DPD ou l'atteinte au statut du DPD »

L'autorité de protection des données (APD)

L'APD peut agir soit à la suite d'une saisie (plainte, requête qui lui a été envoyée), soit d'initiative (ex. : elle a entendu des rumeurs ou elle a connaissance de pratiques non conformes et elle prend la décision de mener une enquête).

L'enquête est menée par le service d'inspection de l'APD qui dispose de pouvoirs d'enquête assez conséquents. Il peut, par exemple, mener des auditions des membres du personnel du responsable du traitement, procéder à des examens sur place, copier ou saisir des données, etc. Dans les pouvoirs d'enquête du service d'inspection, certaines mesures s'apparentent à des perquisitions : les inspecteurs peuvent en effet demander un accès aux locaux du CPAS. En cas de refus, ils peuvent s'adresser à un juge.

Durant cette enquête, des premières sanctions provisoires peuvent être prises. Si le service réunit des preuves suffisantes qui attestent qu'un traitement illégal a eu lieu (traitement qui n'aurait pas dû avoir lieu car il ne disposait pas de base de licéité), il pourrait contraindre l'institution à suspendre ou limiter ce traitement.

À l'issue de l'enquête, trois possibilités peuvent se concrétiser :

1. soit le dossier est classé sans suite et ne conduit pas à des poursuites, des sanctions ;
2. soit le dossier est transmis à la chambre contentieuse de l'APD (organe de jugement de l'APD) ;
3. soit le dossier est transféré au procureur du Roi en cas d'infractions graves, pénales.

La chambre contentieuse de l'APD dispose de toute une série de sanctions, parmi lesquelles :

- la réprimande ;
- ordonner de se conformer à la demande d'une personne concernée (p. ex. : si une personne fait une demande d'accès à ses données et que le CPAS n'y répond pas, l'APD peut ordonner d'y répondre et peut assortir la demande d'astreintes) ;
- l'interdiction temporaire/définitive de traitement[10] ;
- demander la publication de la décision sur son site internet (ce qui peut être désastreux en terme de réputation).

[7] https://www.autoriteprotectiondonnees.be/formulaire-de-communication-des-coordonnees-du-delegue-a-la-protection-des-donnees

[8] https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/2019_data_protection_officer_fr_socsec.pdf

[9] La désignation du DPD par le Conseil de l'action sociale peut être envoyée à l'adresse suivante : dpo@mi-is.be

[10] Qui devrait être plus rare pour les autorités publiques vu qu'elles sont chargées de mener des traitements dans le cadre de leurs missions.

Le juge civil

Au niveau des sanctions, le président du Tribunal de 1re instance peut globalement prendre les mêmes sanctions que l'APD : fin du traitement, limitation dudit traitement, ordonner de respecter les droits des personnes concernées, astreintes. La vraie différence c'est que lui peut ordonner la publicité du jugement dans et en dehors des locaux du responsable du traitement (par ex. : dans les locaux du CPAS, de la maison de repos, aux valves de la commune, par voie de presse…).

Le juge pénal

Le juge pénal a une compétence plus réduite que celle de l'APD ou que du tribunal civil. Il n'est compétent que pour quelques infractions considérées comme graves[11] : traitement illicite (qui n'a pas de base de licéité pour être effectué), traitement sans finalité, non-respect d'un droit d'opposition d'une personne concernée, irrespect d'une injonction de l'APD.

Le juge pénal peut également ordonner la publication du jugement.

[11] Ces infractions sont limitativement énumérées aux art. 222 à 230 de la L. du 30.07.2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (M.B. 05.09.2018).

QUELLES RESPONSABILITÉS POUR LE CPAS (PERSONNE MORALE) EN CAS DE NON-RESPECT DU RGPD ?

Le principe général est que, en cas d'infraction, c'est le responsable du traitement (le CPAS en tant que personne morale de droit public) qui est responsable.

Attention : même lorsqu'une personne physique est désignée pour veiller au respect des principes de protection des données ou pour traiter des données (ex. : l'agent qui effectivement traite des données), cette personne n'est pas responsable du traitement. Elle ne fait qu'agir pour le compte de la personne morale qui demeure responsable.

Il existe cependant deux exceptions à ce principe.

- 1re exception : le cas dans lequel un agent du CPAS va être requalifié en tant que responsable du traitement. Par exemple : un agent du CPAS a accès aux données du Registre national pour des finalités bien déterminées dans le cadre de l'exercice des missions du CPAS, mais il profite de cet accès pour accéder aux données de gens qu'il connaît. Dans un tel cas, il va être personnellement requalifié de responsable du traitement car il a lui-même fixé les objectifs de son traitement de données (par ex., avoir des informations sur son voisin) et les moyens mis en œuvre pour y parvenir (détourner les accès du CPAS). Sa requalification en tant que responsable de traitement implique qu'il est personnellement en charge de la conformité avec la règlementation (sécurité, traitement des données, privacy by design et by default…).

  Cependant, un tel cas de figure nécessite également de s'interroger sur les circonstances qui ont permis à cet agent de détourner les accès. Les mesures de sécurité techniques et organisationnelles étaient-elles suffisantes ? Y a-t-il eu des manquements manifestes du CPAS dans ce domaine ? Le CPAS pourrait également se voir sanctionné si cette violation de données fait suite à des négligences du CPAS en matière de sécurité.
- 2e exception : des sanctions pénales pourraient toucher personnellement un préposé ou un mandataire du responsable du traitement ; mais le CPAS resterait civilement responsable du paiement de l'amende pénale.

Le DPD est-il responsable si le CPAS est condamné pour non-conformité au RGPD ?

La recommandation 4.2017 de la CPVP[12] indique que le responsable du traitement demeure en charge de la conformité avec la réglementation. Sauf exceptions envisagées ci-dessus, le DPD n'est pas responsable de cette conformité.

Les lignes directrices du groupe de l'article 29[13] abondent dans ce sens puisqu'elles indiquent que « *le contrôle du respect du RGPD ne signifie pas que le DPD est personnellement responsable en cas de non-respect de celui-ci* »[14]. Ce n'est donc pas parce qu'il contrôle le fait que le CPAS respecte ou non le RGPD qu'il est responsable en cas de problème.

La décision finale d'un traitement de données revient au responsable de traitement (à la personne morale). Le DPD n'a qu'un rôle de conseil, d'avis. Par analogie, on peut considérer que le DPD est comme un moniteur auto-école qui vous indiquerait de passer un virage en 2e. Si vous le passez en 4e et que vous finissez dans le ravin, le moniteur n'est pas responsable de l'erreur commise.

Si un CPAS passe outre l'avis de son DPD sur un traitement de données et qu'il commet une erreur, c'est le CPAS qui est responsable.

Est-ce que ça veut dire pour autant que le DPD est intouchable ?

Pour la sphère externe, oui. Si l'APD voit qu'un CPAS ne respecte manifestement pas le RGPD, elle va condamner le CPAS. Elle ne peut pas condamner le DPD.

Pour la sphère interne, la réponse est plus nuancée. Le RGPD indique que le DPD ne peut être relevé de ses fonctions ou pénalisé par le responsable de traitement pour l'exercice de ses missions[15]. L'essence de cette disposition est d'éviter qu'un DPD soit sanctionné pour le **bon exercice** de ses missions, pour le fait qu'il ait un œil sur les traitements de données, qu'il mette le doigt sur un traitement qui n'avait pas lieu d'être, pour le fait qu'il ait conseillé ou imposé que la politique de sécurité des données soit réformée.

> *« Le contrôle du respect du RGPD ne signifie pas que le DPD est personnellement responsable en cas de non-respect de celui-ci*

Cela veut-il dire pour autant qu'il ne peut pas être pénalisé pour le **mauvais** exercice de ses missions ? Dans son intervention, Loïck Gérard indique que « non », qu'il s'agirait d'une lecture déraisonnable du RGPD.

L'article 4, al.3 de l'A.R. du 12.8.199316 confirme cette orientation puisqu'il précise que « *les délégués à la protection des données et leurs adjoints éventuels ne peuvent être relevés de cette fonction en raison des opinions qu'ils émettent ou des actes qu'ils accomplissent dans le cadre de l'exercice* ***correct*** *de leur fonction* ».

[12] https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_04_2017.pdf

[13] Groupe de travail « Article 29 » sur la protection des données, Lignes directrices concernant les délégués à la protection des données (DPD) : https://www.cnil.fr/sites/default/files/atoms/files/wp243rev01_fr.pdf

[14] *Ibid*., p.20.

[15] Art. 38.3. du RGPD.

[16] A.R. du 12.08.1993 rel. à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale, M.B., 21.08.1993.

NOUVELLE BOÎTE À OUTILS : les missions des CPAS !

MARIE-CLAIRE THOMAES-LODEFIER
Conseiller expert

Les missions menées par les CPAS sont à l'image de la complexification des parcours de vie et des besoins qui y sont liés. La guidance budgétaire, la formation, la prévention par rapport à la précarité énergétique, l'insertion sociale, l'accompagnement des personnes d'origine étrangère, l'aide médicale urgente, l'accompagnement au logement… ne sont que quelques exemples de services rendus. En quelque sorte, un miroir grossissant de ce que la société génère aujourd'hui. Cette étendue de missions s'est aussi accompagnée d'une complexification de l'administration et du métier de travailleur social car, derrière chaque dispositif, il y a des textes règlementaires. Les CPAS sont devenus des institutions socio-juridico-administratives qu'il convient de comprendre pour bien en appréhender les richesses mais aussi les limites.

C'est la raison pour laquelle l'équipe de la Fédération des CPAS s'est penchée sur les missions des CPAS dans leur évolution et sur les arcanes du droit à l'intégration sociale et de l'aide sociale, sous la coordination de Marie-Claire Thomaes-Lodefier, Juriste et Conseiller expert au sein de la Fédération. Cet ouvrage est un outil indispensable aux acteurs des CPAS, au premier rang desquels les mandataires, mais aussi les grades légaux, travailleurs sociaux et travailleurs « administratifs ».