LE RGPD
COMME BOUSSOLE POUR LE QUOTIDIEN!

JUDITH DUCHÊNE
Conseillère

Deux évènements récemment organisés par la Fédération des CPAS[1] ont permis de faire, une fois de plus, le point sur la désignation des délégués à la protection des données (DPD) au sein des CPAS wallons et sur la responsabilité du CPAS dans le cadre du RGPD. Un article publié précédemment[2] reprenait déjà les principaux enjeux, les modalités concrètes et la responsabilité du CPAS pour la désignation d'un DPD.

L'actualité de la nécessité, pour les CPAS, de remplir et renvoyer avant fin octobre le questionnaire annuel sur les normes minimales de la Banque Carrefour de la Sécurité sociale (BCSS) nous donne la possibilité d'insister encore une fois sur l'importance de cette thématique.

Par le biais de l'intervention de J. Folon à la Plateforme du 7 septembre, nous listerons ici une série de questions fondamentales que chaque CPAS doit se poser dans le cadre de la désignation d'un DPD eu égard aux obligations inscrites dans le RGPD et à sa responsabilité en tant que responsable de traitement.

Une feuille de route assez télégraphique mais qui peut peut-être servir de boussole pour s'orienter et se mettre en chemin.

L'article 37 du RGPD rend obligatoire, pour toute autorité publique[3], la désignation d'un DPD. Le CPAS étant une autorité publique, il doit obligatoirement, depuis le 25 mai 2018, désigner un DPD. L'absence de désignation d'un DPD ou l'atteinte à son statut peut donc être sanctionnée en tant qu'infraction de non-conformité au RGPD.

Cette obligation est également reprise dans la loi organique de la BCSS[4] et la complexité des normes minimales qui s'imposent aux institutions de sécurité sociale montre, dans la pratique, qu'il s'agit véritablement d'un métier à part entière, mobilisant des compétences techniques et juridiques précises, et dont le CPAS ne peut plus ignorer à quel point il est un métier essentiel pour l'institution.

Que vous ayez déjà désigné un DPD ou que vous soyez en passe de le faire, nous espérons que cette check-list de questions à se poser attirera votre attention sur certains éléments et permettra de consolider la fonction du DPD au sein de chaque CPAS.

Un DPD? Mais comment le choisir?

1. Sur la base de ses compétences

- Quelle(s) formation(s) votre DPD a-t-il suivie(s)?
- Êtes-vous capable de démontrer que votre DPD (interne ou externe) a les qualités suffisantes pour être DPD?

1 Séance d'information sur le questionnaire 2021 sur les normes minimales de la BCSS, 7.9.2021 ; Plateforme DG et DPD de CPAS, 21.9.2021.

2 J. Duchêne, *Délégué à la protection des données : ses responsabilités et celles du CPAS !*, *CPAS+*, 6-7.2019, pp.10-13.

3 L'art. 5 de la L. du 30.7.2018 rel. à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (M.B. 5.9.2018) donne une définition de ce qui doit être entendu par « autorité publique ».

4 Art. 4, § 5 de la L. du 15.1.1990 organique de la BCSS : « *Toute autorité publique, personne physique et organisme public ou privé qui a accès aux données d'identification des registres Banque-Carrefour ou en obtient la communication, conformément au § 4, désigne, parmi ses membres du personnel ou non, [un délégué à la protection des données, ...* ».

Art. 24 de la L. du 15.1.1990 organique de la BCSS : « *Toute institution de sécurité sociale désigne, au sein de son personnel ou non, un délégué à la protection des données et communique son identité à la Banque-carrefour* ».

Art. 4 de l'A.R. du 12.8.1993 rel. à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale « *Après leur désignation, l'identité du délégué à la protection des données et de ses adjoints éventuels dans les institutions qui appartiennent à un réseau secondaire est communiquée à l'institution gérant le réseau secondaire concerné* ».

Normes minimales de la BCSS qui doivent être respectées par le CPAS (et donc vérifiées et mises en œuvre par le DPD => donne un éclairage sur une partie des tâches qui doivent être menées par le DPD): https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/mnm_normes_minimales.pdf

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 (art. 39), à savoir notamment :
  - 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.

- Une décision motivée de la direction a-t-elle été prise et insérée dans le « dossier » RGPD ?

Dans le cadre du RGPD, le CPAS doit pouvoir à tout moment prouver qu'il respecte bien le règlement (principe d' « accountability »). Il est donc indispensable de mettre en place un dossier permettant de documenter l'ensemble des process relatifs à la mise en conformité de l'institution. Ce dossier ne sera jamais fini, puisqu'il évoluera au gré des nouveaux projets que se donnera l'institution, des changements de règlementations, des avis émis par l'Autorité de Protection des Données (APD), de la jurisprudence…

- Cette décision précise-t-elle bien les raisons du choix et reprend-elle les éléments nécessaires afin de démontrer la compétence du candidat ?

La décision dans laquelle le CPAS décide de désigner une telle personne en tant que DPD doit être motivée : il s'agit d'expliquer pourquoi cette personne a été choisie et de démontrer sa compétence pour exercer la fonction.

2. Évitez les conflits d'intérêts!

- Avez-vous tenu compte des incompatibilités de fonction avec la fonction de DPD ?

Le CPAS doit veiller à ce que le DPD n'exerce pas, au sein du CPAS, une fonction qui l'amène à être juge et partie. Le DPD ne peut donc pas être une personne qui, au sein de l'institution, prend des décisions relatives à des traitements de données ou aux mesures de sécurité qui encadrent ces traitements. Il ne peut donc pas être : un grade légal, un directeur du personnel, un responsable informatique.

- Avez-vous tenu compte, pour un DPD à temps partiel, des éventuels conflits d'intérêt avec son autre fonction ?

Lorsqu'un DPD est engagé à temps partiel, il faut qu'il soit clairement précisé dans le contrat de travail le temps et les jours consacrés à l'activité de DPD et le temps/les jours consacrés aux autres activités.

Il en va de même pour un DPD mutualisé entre plusieurs entités. Le temps/les jours consacrés à chacune des entités doivent être précisés.

Le DPD à temps partiel ne peut pas se trouver en situation de conflit d'intérêt entre son activité de DPD et son autre activité au sein de l'institution.

- Avez-vous inséré votre raisonnement au sujet des conflits d'intérêts dans la décision motivée de la désignation du DPD ?

3. Comment acter la décision de nomination?

- Pour la désignation du DPD du CPAS, avez-vous pris une décision dûment motivée au sein du conseil de l'action sociale (CAS) ?
- Avez-vous inséré une copie de cette décision dans le dossier RGPD ?
- Avez-vous notifié cette décision à l'APD[5] ? À la BCSS[6] ? Au SPP IS[7] ?

S'il s'agit d'un DPD pour plusieurs entités, chaque CAS doit prendre une décision de désignation et notifier celles-ci à l'APD, la BCSS et au SPP IS.

- Une copie de ces notifications a-t-elle été insérée dans le dossier RGPD ?

4. Garantir l'indépendance du DPD

- Un contrat de travail et/ou une description de fonction ont-elles été rédigées pour le DPD ?

Le RGPD définit les missions du DPD mais il est intéressant de préciser concrètement, au sein de l'institution, ce qu'il va faire et comment il va travailler.

Pour préciser le contenu de sa fonction, il faut également se référer à ce qui est attendu du DPD dans le cadre de la législation relative à la BCSS et à la sécurité de l'information dans les institutions de sécurité sociale. Le questionnaire sur les normes minimales de la BCSS peut également servir de ressource.

5 https://www.autoriteprotectiondonnees.be/notifier-delegue-a-la-protection-des-donnees

6 https://ksz-bcss.fgov.be/fr/protection-des-donnees/en-pratique/delegue-a-la-protection-des-donnees-dpo

7 La désignation du DPD par le CAS peut être envoyée à l'adresse suivante : dpo@mi-is.be.

- Le contact avec l'APD est-il prévu dans ce document ?
- Le DPD peut-il effectivement choisir ce qu'il contrôle ?

L'indépendance du DPD est importante. Il doit pouvoir librement choisir ce qu'il veut contrôler au sein de l'institution et disposer ainsi d'un « droit de déranger » : le droit d'aller voir ce qui se passe dans n'importe quel processus de traitement de données à caractère personnel, dans les pratiques de protection de ces traitements, le droit d'aller poser des constats qui mettent en cause les manières de faire en interne.

- Le DPD rapporte-t-il à la plus haute autorité hiérarchique ?

Le DPD doit pouvoir être en contact direct avec le plus haut niveau de hiérarchie du CPAS et être informé en amont de toutes les décisions concernant les traitements de données à caractère personnel au sein de l'institution.

Le soutien de la hiérarchie est absolument essentiel : si la direction ne s'intéresse pas au RGPD, personne ne s'y intéressera.

Différentes actions peuvent être mises en place pour concrétiser cela :

- faire participer le DPD au CODIR (ou à un CODIR élargi) lorsque celui-ci implique des décisions relatives aux traitements de données à caractère personnel ;
- instaurer une proximité de travail entre le DG et le DPD : bureaux à proximité, intégration du DPD dans l'équipe de la direction générale, présentation de l'institution au DPD lors de sa désignation et présentation du DPD à toutes les équipes, envoi d'une note de service aux agents expliquant la fonction du DPD, remise au DG d'un bilan hebdomadaire du travail réalisé par le DPD, organisation de rencontres entre le DPD et chaque chef de service…

Il est également important de pouvoir sensibiliser le CAS sur les questions relatives à la protection de la vie privée, à la sécurité et aux traitements des données. Un rapport annuel du travail du DPD pourrait leur être envoyé et présenté afin de donner de la visibilité à la fonction et au travail accompli.

- Le DPD est-il indépendant par rapport au pouvoir politique ?

5. Associer le DPD aux décisions concernant les données à caractère personnel (DACP)[8]

- Le DPD est-il informé de tous les projets touchant aux DACP ?
- Le DPD participe-t-il au processus de décision touchant à des DACP ?
- L'avis du DPD est-il systématiquement demandé lors de projets liés aux DACP ?
- Les décisions de la direction tiennent-elles compte systématiquement de l'avis du DPD ?

Il convient de noter, à cet égard, que DPD et direction peuvent ne pas être d'accord. Le rôle du DPD est de donner un avis et de conseiller. La direction décide, en connaissance de cause et peut, sur base d'autres arguments, ne pas suivre l'avis du DPD.

Comme pour toute action relevant de la mise en conformité au RGPD, il convient de documenter le travail et de consigner l'avis du DPD et la décision argumentée de la direction dans le dossier RGPD.

- Le DPD participe-t-il au « privacy by design » ?

Le « privacy by design » est le fait que le responsable de traitement (CPAS) doit penser à la sécurité de celui-ci dès qu'il envisage un traitement de données, ainsi que dans toutes les étapes de sa mise en œuvre.

- Le DPD participe-t-il aux analyses d'impact ?

Pour chaque traitement de données susceptible d'engendrer des risques élevés pour les droits et libertés des personnes concernées, une analyse d'impact relative à la protection des données doit être menée.

6. Mettre en place l'information interne

- Le DPD a-t-il pu mettre en place une formation du personnel relative aux enjeux des traitements de données à caractère personnel ?
- Les documents d'information en matière de ressources humaines ont-ils été réalisés et communiqués : information sur les DACP, charte informatique, clauses de confidentialité… ?

7. Conclusion

La bonne collaboration entre le DG du CPAS, le DPD et les membres du comité de direction (CODIR) fait partie des indispensables dans le cadre de la mise en œuvre du RGPD. Le DPD est notamment investi d'un rôle de conseil et d'information de la hiérarchie par rapport aux obligations du CPAS. Il doit pouvoir être en contact direct avec elle, afin d'éviter que ses avis soient reformulés ou dilués à chaque échelon de l'administration.

Le DPD doit également pouvoir compter sur le soutien de la hiérarchie pour être en mesure d'assurer ses missions, pour disposer du temps nécessaire pour le faire et aller se former, pour que le relais d'information de tous les projets/de toutes les actions du CPAS soit assuré vers lui, afin qu'il puisse en analyser les impacts éventuels sur la protection des données à caractère personnel.

Il s'agit d'un fameux défi car c'est toute l'organisation interne d'un CPAS qui peut être repensée face à ces nécessités. Le RGPD constitue très certainement une excellente base pour entamer ce travail car il permet de recenser tous les flux d'informations (papier et numériques) qui circulent dans l'institution, mais implique également de porter une attention globale sur la sécurité (sécurité des bâtiments, localisation des serveurs, emplacement des dossiers, des archives…).

Il se révèle donc être un outil efficace pour la gestion du quotidien. ■

[8] Pistes proposées dans les encadrés précédents.