Recommandation n° 04/2017 du 24 mai 2017

Objet: Recommandation relative à la désignation d'un délégué à la protection des données conformément au Règlement général sur la protection des données (RGPD), en particulier l'admissibilité du cumul de cette fonction avec d'autres fonctions dont celle de conseiller en sécurité (CO-AR-2017-008)

La Commission de la protection de la vie privée ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après LVP), en particulier l'article 30 ;

Vu le rapport de Monsieur Willem Debeuckelaere;

Émet, le 24 mai 2017, la recommandation suivante:

I. INTRODUCTION

1. Le Règlement général sur la protection des données (ci-après RGPD)[1] est entré en vigueur le 24 mai 2016 et sera d'application à dater du 25 mai 2018.

2. Dans le chapitre IV du RGPD qui énonce les obligations des responsables de traitement et des sous-traitants, la section IV est entièrement consacrée au *délégué à la protection des données*. Plus spécifiquement, l'article 37 détaille les cas dans lesquels la désignation du délégué à la protection des données est obligatoire ainsi que les modalités de cette désignation ; l'article 38 encadre la fonction même de délégué à la protection des données (statut) et l'article 39 décrit quelles sont ses missions. Quelques autres articles du RGPD viennent compléter l'encadrement de cette fonction nouvelle[2].

3. Immédiatement après l'adoption du RGPD, les autorités de protection des données ont identifié la question du délégué à la protection des données comme prioritaire. Elles ont incité les responsables de traitement et sous-traitants à vérifier rapidement si oui ou non ils sont juridiquement tenus de désigner un délégué à la protection des données en application de l'article 37.1. du RGPD ainsi qu'à procéder aux engagements ou à programmer les formations nécessaires.[3] Réunies au sein du Groupe de l'Article 29, elles ont également encouragé la désignation volontaire de tels délégués et proposé des lignes directrices d'interprétation commune des articles pertinents du RGPD ainsi que formulé un certain nombre de recommandations (best practice)[4].

4. Outre les questions récurrentes auxquelles elle a déjà répondu par la voie de FAQ sur son site Internet[5] (et pour la réponse auxquelles elle s'appuie sur le travail d'interprétation commune du groupe de l'Article 29 déjà cité), la CPVP reçoit régulièrement la question de savoir si le

---

1 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *JO, L 119, 4.5.2016, pp. 1–88.*

[2] L'article 35 relatif à l'analyse d'impact relative à la protection des données qui prévoit que le responsable de traitement demande conseil au délégué à la protection des données si un tel délégué a été désigné (§2) ; les articles 13 et 14 relatifs à l'information de la personne concernée : les coordonnées du délégué doivent lui être communiquées et les articles 33 et 34 relatifs à la notification des failles de sécurité à l'autorité de protection des données et à la personne concernée : les coordonnées du délégué doivent leur être communiquées.

[3] Voy. par exemple le plan d'action en 13 étapes développé par la CPVP : https://www.privacycommission.be/fr/news/reglement-general-sur-la-protection-des-donnees

[4] Groupe de l'Article 29, Guidelines on Data Protection Officers (« DPOs »), WP 243 du 13 décembre 2016, révisé après consultation publique et adopté dans sa version définitive le 5 avril 2017 .

[5] Rubrique FAQ sur le site de la CPVP : https://www.privacycommission.be/fr/faq-page

« conseiller en sécurité »[6] que doivent désigner certaines institutions, organismes et autres entités en application de différentes règlementations belges peut devenir le délégué à la protection des données - exigé pour toute autorité et organisme publics notamment (37.1. du RGPD) -. Peut-il exercer cumulativement les fonctions de conseiller en sécurité et de délégué à la protection des données et, le cas échéant, à quelles conditions ?

5. La présente recommandation a pour objectif de guider les responsable de traitement et les sous-traitants dans leur analyse et leur choix d'un délégué à la protection des données dans le respect du RGPD (voy. le point III). Compte tenu des nombreuses questions que la CPVP reçoit quant au cumul de cette fonction avec celle de « conseiller en sécurité », une attention particulière, mais non exclusive, sera accordée à cet aspect dans la présente recommandation

II. RETROACTES

Les prémisses de la fonction dans la directive 95/45/CE : le détaché à la protection des données

6. L'article 18.2. de la directive 95/46/CE a certes, dès 1995, introduit la fonction de « détaché à la protection des données ». Concrètement, sur la base de cette disposition, les Etats membres ont pu – sans donc y être obligés -, par la voie législative, prévoir que les responsables de traitement qui désignent un détaché à la protection des données au sens de cet article 18.2. sont dispensés de la déclaration préalable de traitement auprès de l'autorité de contrôle (soit la déclaration visée à l'article 17 de la LVP). Aux termes de l'article 18.2. précité, ce détaché à la protection des données doit exercer ses missions en toute indépendance et tenir un registre des activités de traitement de données interne au responsable de traitement.

7. Un certain nombre d'Etats membres de l'Union européenne ont fait usage de cette faculté et ont prévu la fonction de « détaché à la protection des données » dans leur législation nationale de transposition de la directive 95/46/CE non sans le dénommer de diverses manières et lui confier des missions complémentaires à celles énoncées dans la directive 95/46/CE. Ces missions complémentaires varient par ailleurs d'une législation nationale à l'autre.

8. On parle ainsi actuellement, sans que l'énumération ne soit exhaustive, de « Correspondants Informatique et Liberté » (CIL) en France, de « Chargé de la protection des données » au Grand-Duché de Luxembourg, de « Functionaris voor de gegevensbescherming » aux Pays-

[6] Voy. les points 9 à 15 ci-après.

Bas, de « Data Protection Officer » au Royaume-Uni, et déjà de « Délégué à la protection des données » au sein des institutions de l'Union européenne.

La fonction de préposé à la protection des données et de conseiller en sécurité en droit belge

9. En droit belge, l'article 17bis de la loi Vie privée (LVP) a introduit la fonction de « préposé à la protection des données » énonçant que :

> *« Le Roi détermine, après avis de la Commission de la protection de la vie privée, les catégories de traitements qui présentent des risques particuliers au regard des droits et libertés des personnes concernées et fixe, également sur proposition de la Commission de la protection de la vie privée, des conditions particulières pour garantir les droits et libertés des personnes concernées.*
> *Il peut en particulier déterminer que le responsable de traitement désigne un* ***préposé à la protection des données*** *chargé d'assurer, de manière indépendante, l'application de la présente loi et de ses mesures d'exécution.*
> *Le Roi détermine par arrêté délibéré en Conseil des ministres, après avis de la Commission de la protection de la vie privée, le statut du préposé à la protection des données ».*

10. Contrairement à l'article 18.2. de la directive 95/46/CE, l'article 17bis de la loi Vie privée ne lie pas « exemption de déclaration » et « préposé à la protection des données ».[7] Le responsable de traitement qui désigne un préposé à la protection des données n'est en rien dispensé de déclarer les traitements auxquels il procède auprès de la CPVP.

L'article 17bis de la loi Vie privée lie par contre la fonction de « préposé à la protection des données » à la mise en œuvre de traitements présentant des risques particuliers au regard des droits et libertés des personnes concernées (alinéa 1er).

Le législateur belge s'est ici encore écarté des prescrits tant de l'article 18§2 précité que de l'article 20 de la Directive 95/46/CE. Aux termes de cette dernière disposition, les Etats membres précisent les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées et veillent à ce que ces traitements soient examinés avant leur mise en œuvre (§1er), en d'autres termes, fassent l'objet d'autorisations préalables de traitement.

[7] Les termes « préposé à la protection des données » à l'article 17bis de la Loi Vie privée renvoient à ceux de « détaché à la protection des données » de l'article 18 § 2 de la Directive 95/46/CE.

11. La CPVP a plusieurs fois appelé de ses vœux l'adoption de cet arrêté royal générique mentionné à l'article 17bis de la LVP. Celui-ci n'a cependant jamais été adopté.

12. Plusieurs législations spécifiques n'en n'ont pas moins prévu la désignation obligatoire d'une personne exerçant cette fonction, le plus souvent cumulée à une fonction de conseiller ou de responsable en sécurité selon la terminologie retenue par la législation concernée sans que pourtant, comme déjà mentionné, le statut de ce préposé n'ait été plus amplement défini.

13. A titre d'exemples, non exhaustifs, citons :
    a. La *Loi relative au Registre national* qui impose à *« chaque autorité publique, organisme public ou privé qui a obtenu l'accès aux informations du Registre national ou la communication des dites informations [de] désigne[r] au sein ou en – dehors de son personnel,* ***un consultant en sécurité de l'information et en protection de la vie privée*** *qui remplit entre autres la fonction du préposé à la protection des données visé à l'article 17bis de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. (…) ».*[8]

    b. La Loi du 19 mai 2010 portant création de la Banque carrefour des véhicules qui prévoit en son article 28 que *« Chaque service désigne, au sein ou en dehors de son personnel, un* ***responsable en sécurité de l'information et en protection de la vie privée*** *qui remplit également la fonction de préposé à la protection des données visée à l'article 17bis de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. L'identité de ce responsable est communiquée au comité sectoriel et au service de gestion ».*

    c. L'Arrêté royal du 6 décembre 2015 relatif aux **conseillers en sécurité et en protection de la vie privée** et à la plate-forme de la sécurité et de la protection des données pris en exécution de la Loi sur la fonction de police (article 44/3, § 1er, alinéas 5, 3°, et 8, et § 2, alinéa 2.).

14. D'autres législations exigent la désignation d'un « conseiller en sécurité » sans qu'ici non plus un encadrement légal général n'existe :

    a. Lors de l'élaboration de la *loi organique de la Banque-Carrefour de la sécurité sociale*, le législateur a consacré une attention particulière à la protection de la Banque carrefour, de son réseau ainsi que des données personnelles qui sont échangées via

[8] Loi du 8 août 1983 organisant un registre national des personnes physiques, *M.B.*, 21 avril 1984.

ce réseau notamment en instituant un « conseiller en sécurité » au sein de chaque institution sociale.[9]

b. La *réglementation hospitalière* impose elle aussi la nomination dans les hôpitaux d'un « conseiller en sécurité » chargé de conseiller le responsable de la gestion journalière au sujet de tous les aspects de la sécurité de l'information.[10]

c. Aux termes de l'arrêté royal relatif aux conseillers en sécurité institués par la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral, l'intégrateur de services fédéral ainsi que tout service public participant doivent désigner un conseiller en sécurité[11].

d. Au niveau régional également de telles exigences existent. Aux termes du décret flamand du 18 juillet 2008 relatif à l'échange électronique de données administratives, toute instance qui gère une source authentique de données contenant des données à caractère personnel, toute instance qui reçoit ou échange des données à caractère personnel électroniques, et toute entité qui est désignée conformément à l'article 4, § 3, et traite des données à caractère personnel, désigne un conseiller en sécurité (article 9). [12]

15. Pour couvrir ces différentes variantes, le terme général de « conseiller en sécurité » sera utilisé dans la suite de cette recommandation. Si, comme mentionné, un encadrement légal général n'existe pas, la description de la fonction et le statut de conseiller en sécurité de l'arrêté royal du 12 août 1993 (conseiller en sécurité des institutions de sécurité sociale) sont communs à plusieurs des textes susmentionnés (arrêté royal relatif à l'intégrateur de services fédéral, la Vlaamse besluit du 15 mai 2009, …).

---

[9] Voy. article 24 de la Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, *M.B.*, 22 février 1990. Depuis son adoption, cette législation a fait l'objet de nombreuses modifications. Une version coordonnée et mise à jour de la loi est disponible sur le site de la Banque-carrefour de la sécurité sociale à l'adresse http:// http://ksz-bcss.fgov.be. Voy. en particulier l'arrêté royal du 12 août 1993 relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale, M.B., 21 août 1993.

[10] L'Annexe A Normes générales applicables à tous les établissements visés par l'Arrêté royal du 23 octobre 1964 portant fixation des normes auxquelles les hôpitaux et leurs services doivent répondre stipule : « Le maître du fichier [le responsable du traitement] désigne un conseiller en sécurité chargé de la sécurité de l'information. Le conseiller en sécurité conseille le responsable de la gestion journalière au sujet de tous les aspects de la sécurité de l'information. (…) », *M.B.*, 7 novembre 1964.

[11] Section 5: articles 20-23 de l'arrêté royal du 17 mars 2013 relatif aux conseillers en sécurité institués par la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral, *M.B.*, 22 mars 2013.

[12] Voy. Également: Besluit van de Vlaamse Regering van 15 mei 2009 betreffende de veiligheidsconsulenten, vermeld in artikel 9 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.

Aux termes de cette description, le conseiller en sécurité a une mission d'avis, de stimulation, de documentation et de contrôle.

L'article 3 de l'arrêté royal du 12 août 1993 mentionne ainsi que :

- Le service chargé de la sécurité de l'information, est placé sous la direction du conseiller en sécurité.

- Ce service conseille (par voie d'avis) au sujet de tous les aspects de la sécurité de l'information définie comme les stratégie, règles, procédures et moyens de protection de tout type d'information, tant dans les systèmes de transmission que dans les systèmes de traitement en vue de garantir la confidentialité, la disponibilité, l'intégrité, la fiabilité, l'authenticité et l'irréfutabilité de l'information[13].

- Le service chargé de la sécurité de l'information promeut également le respect des règles de sécurité imposées par une disposition légale ou règlementaire ou en vertu d'une telle disposition, ainsi que l'adoption par les personnes employées dans l'institution concernée d'un comportement favorisant la sécurité.

- Ce même service rassemble la documentation utile à ce sujet.

- Enfin, le service chargé de la sécurité de l'information veille au respect dans l'institution, des règles de sécurité imposées par une disposition légale ou règlementaire ou en vertu d'une telle disposition. Toutes les infractions constatées sont communiquées par écrit et exclusivement au responsable de la gestion journalière, accompagnées des avis nécessaires en vue d'éviter de telles infractions à l'avenir.

- S'agissant de son statut, le conseiller en sécurité est désigné après avis du Comité de surveillance qui vérifie (article 4) que le conseiller dispose d'une connaissance suffisante et du temps nécessaire pour pouvoir mener cette mission à bien. Le Comité vérifie également qu'il n'exerce pas d'activités qui pourraient être incompatibles avec cette mission. Le conseiller en sécurité ne peut être relevé de sa fonction en raison des opinions qu'il émet ou des actes qu'il accomplit dans le cadre de l'exercice correct de ses fonctions et doit être placé sous l'autorité fonctionnelle directe du responsable de la gestion journalière.[14]

[13] Voy. l'article 1, 9° de l'arrêté royal du 12 août 1993 précité.

[14] Il s'agit du Comité visé à l'article 37 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale.

La pratique du RSSI (CISO)

16. Sans y être toujours légalement tenus, nombre d'organisations et entreprises ont par ailleurs désigné un **Responsable de la sécurité des systèmes d'information (RSSI)** parfois plus connu sous la dénomination anglaise de ***Chief information security officer* (*CISO*).**

L'orientation nouvelle du RGPD

17. Le RGPD abandonne le concept du détaché à la protection des données au rôle relativement limité et fait du « délégué à la protection des données » une des pierres angulaires du régime d'accountability sur lequel il s'appuie. Il harmonise tant la terminologie que les critères et modalités de désignation, du statut et des missions de ces délégués à la protection des données. Leur rôle aux termes du RGPD va bien au-delà de ce qui est prévu par la directive 95/46/CE et de ce qu'ont pu prévoir les différentes législations nationales de transposition de cette directive ou d'autres législations nationales sectorielles. Enfin, à la différence de la directive 95/46/CE, le RGPD vise également les sous-traitants et plus uniquement les responsables de traitement.

18. Compte tenu des missions qui lui sont attribuées, le délégué à la protection des données peut faciliter la conformité au RGPD dans tous ses aspects (accountability) et devenir également un véritable outil de compétitivité pour les entreprises.

III. OBJECTIF DE LA RECOMMANDATION

A qui s'adresse cette recommandation ?

19. Désigner un délégué à la protection des données est, dans un nombre de cas listés à l'article 37.1 du RGPD, une obligation et, dans les autres cas, une faculté *tant pour les responsables de traitement que pour les sous-traitant* auxquels s'applique le RGPD sauf si la législation d'un état membre devait ajouter des cas obligatoires par voie légale (art. 37.4.).

Plus précisément :

- S'agissant du secteur public, la désignation d'un délégué à la protection des données est obligatoire pour les autorités publiques et les organismes publics à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle (article 37.1.a).

- Pour le secteur privé, la désignation d'un délégué à la protection des données est une faculté sauf dans les 2 cas prévus aux articles 37.1. b) et c) du RGPD.

20. Aux termes de l'article 83 du RGPD, les violations des obligations incombant au responsable de traitement et au sous-traitant en vertu des articles 37, 38 et 39 relatifs au délégué à la protection des données font l'objet d'amendes administratives pouvant s'élever jusqu'à 10.000.000 EUR ou, dans le cas d'une entreprise, jusqu'à 2% du chiffre d'affaire mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

21. Le responsable de traitement ou le sous-traitant demeurent en charge de la conformité avec la règlementation en matière de protection des données et doivent être en mesure de démontrer cette conformité. Le délégué n'est pas responsable de cette conformité. Ce sont également les responsables de traitement et les sous-traitants qui peuvent être sanctionnés pour violation du RGPD,

Quels sont la portée et l'objectif de cette recommandation ?

22. Outre la question spécifique énoncée au point 4 ci-dessus, la question plus générale se pose de savoir si les responsables de traitement et sous-traitants concernés peuvent, pour se conformer au RGPD, confier la tâche de délégué à la protection des données à l'une ou l'autre personne exerçant par ailleurs une autre fonction dans l'institution, organisme ou entreprise. En d'autres termes, une même personne peut-elle exercer la fonction de délégué à la protection des données et une autre fonction (préexistante) ?

23. Ou, écrit encore différemment, le conseiller en sécurité des institutions de sécurité sociale, des hôpitaux ou encore du Registre national peut-il en devenir le délégué à la protection des données ? Mais aussi : le Compliance Officer requis dans le secteur des banques et assurances peut-il aussi exercer la fonction de délégué à la protection des données. Qu'en est-il pour le directeur des ressources humaines, le Risk manager, le responsable du service informatique ou encore la personne identifiée elle-même comme responsable de traitement ou sous-traitant etc. ?

24. La présente recommandation n'a pas pour objectif de répondre à chacune de ces questions, ni à fournir une réponse à chacun de ces scénarios ni à tout autre qui pourrait se présenter en fonction de l'organisation interne de l'autorité publique, de l'organisme public ou plus généralement de tout responsable de traitement et sous-traitant concernés.

La CPVP n'examinera donc pas aux termes de cette recommandation la compatibilité du cumul de ces différentes fonctions avec celle du délégué à la protection des données prévue par le RGPD, ni sur le plan de la compatibilité des textes légaux encadrant le cas échéant

l'une ou l'autre de ces fonctions, ni sur le plan de l'exercice pratique de ces fonctions, celui-ci pouvant par ailleurs varier d'un responsable de traitement et sous-traitant à l'autre.

25. Pour plusieurs raisons, la CPVP ne peut en effet s'engager dans cette voie :

    a. Aux termes du RGPD, l'autorité de protection des données n'a pas reçu la compétence de valider le choix de son délégué à la protection des données par le responsable de traitement ou le sous-traitant. A cet égard, la notification à l'autorité de protection des données des coordonnées du délégué à la protection des données prévue à l'article 37.7 n'est en aucune façon à considérer comme une forme de demande d'accord ou de validation de la DPA sur cette désignation. Une telle approche serait contraire au principe de l'accountability.

    b. Une nécessaire flexibilité doit être laissée aux responsables de traitement et sous-traitant dans la manière dont ils souhaitent organiser les tâches et rôles de chacun en leur sein. Un modèle organisationnel unique ne doit pas être imposé.

    c. La CPVP doit conserver toute son indépendance dans la perspective de contrôles qu'elle serait amenée à opérer, par exemple à la suite de plaintes à l'encontre du responsable de traitement ou du sous-traitant ou d'initiative. Ces responsables de traitement ou sous-traitants ont-ils désigné un délégué à la protection des données dès lors qu'ils y sont tenus ? Ce délégué est-il effectivement indépendant ? Présente-il les qualifications requises ? Dispose-t-il de suffisamment de temps pour exercer effectivement ses missions ?

26. La CPVP ne mesure pas moins l'importance de donner certains éléments de guidance aux responsables de traitement et sous-traitants concernés pour les aider à décider à qui la fonction du délégué à la protection peut être confiée dans le respect du RGPD. La CPVP leur recommande à cet égard de documenter leur analyse et le choix final opérés.

27. Elle rappelle aussi que le RGPD autorise à recourir à un délégué externe à l'entité (article 37.3. du RGPD et art. 37.6. du RGPD).

28. Compte tenu toutefois, comme déjà mentionné, du nombre de questions adressées à la CPVP quant à l'admissibilité du cumul de la fonction de délégué à la protection des données avec celle de conseiller en sécurité (voy. supra), la présente recommandation mettra en lumière les grandes différences entre ces deux fonctions, sans toutefois prétendre à l'exhaustivité.

IV. LE DELEGUE A LA PROTECTION DES DONNEES DANS LE RGPD

29. C'est à l'aune de la fonction de délégué à la protection des données telle que décrite par le RGPD que le responsable de traitement et le sous-traitant qui sont tenus ou souhaitent désigner un délégué à la protection des données doivent examiner la possibilité du cumul de cette fonction avec une autre ou la transition d'une fonction à l'autre.[15]

30. S'agissant du délégué volontairement désigné par le responsable de traitement ou le sous-traitant, cette désignation volontaire est encouragée par le Groupe de l'Article 29. Si il ou elle est désigné(e) en tant que tel et dénommé(e) « délégué à la protection des données », l'ensemble des exigences du RGPD devront être respectées. Les articles 37 à 39 s'appliqueront de la même façon que si sa désignation avait été obligatoire.

31. Par le passé, la CPVP a développé une jurisprudence[16] en application de laquelle elle opère une distinction nette entre les fonctions de conseiller en sécurité et de préposé à la protection des données tout en ne s'opposant pas à ce qu'une seule personne cumule les deux fonctions pour autant que la loi lui garantisse l'indépendance indispensable à l'accomplissement de cette double tâche:

    a. *« le conseiller en sécurité doit veiller à la sécurité des applications et à la prise des mesures techniques et organisationnelles aptes à garantir le respect de la confidentialité des données et veiller aux contrôles d'accès et autre. L'article 16 de la Loi Vie privée impose en effet la prise de mesures de sécurité adéquates (principe de sécurité). Par ailleurs, la nécessité de veiller lors de chaque traitement au respect de l'ensemble des principes qui fondent le régime de protection des données à caractère personnel (finalité, proportionnalité, droits de la personne concernée) rend nécessaire l'accomplissement d'une autre fonction : celle de « préposé à la protection des données ». Cette notion couvre, on l'a vu, d'autres compétences que celle de veiller à la seule sécurité des données mais comprend également le devoir « d'assurer de manière indépendante l'application de la présente loi et de ses mesures d'exécution »,*

[15] Quant aux fonctions requises par la règlementation, elles demeurent d'application tant que le législateur n'a pas, le cas échéant, modifié les textes.

[16] Avis 43/2003 relatif au projet d'arrêté royal portant exécution de l'article 6 § 3 de la loi du 2 juin 198 portant création d'un Centre d'information et d'avis sur les organisations sectaires nuisibles et d'une cellule administrative de coordination de la lutte contre les organisations sectaires nuisibles). Aux termes de l'arrêté royal adopté, les tâches du préposé à la protection des données (Chapitre III – article 6) sont limitées aux seuls aspects de la sécurité des données (Arrêté royal du 13 juillet 2006 portant exécution de l'article 6 § 3 de la loi du 2 juin 1998 portant création d'un centre d'information et d'avis sur les organisations sectaires nuisibles et d'une cellule administrative de coordination dans la lutte contre les organisations sectaires nuisibles, *M.B.*, 16 août 2006).

ce qui signifie outre le contrôle du caractère adéquat des mesures de sécurité, celle du contrôle du respect des principes de légitimité, de proportionnalité et du droit d'accès des personnes concernées. La Commission, si elle estime fondée la distinction des deux fonctions, ne s'oppose cependant pas à ce qu'une seule personne cumule les deux fonctions pour autant que la loi lui garantisse l'indépendance indispensable à l'achèvement de cette double tâche (…) ».[17]

Cette jurisprudence ne peut être utilisée aujourd'hui pour conclure que dans tous les cas, le conseiller en sécurité en fonction à l'heure actuelle peut de façon automatique être le délégué à la protection des données de demain. Comme déjà mentionné, c'est désormais à l'aune de la fonction telle que décrite par le RGPD que cet aspect doit être examiné.

32. Sans répéter l'ensemble des explications fournies par le Groupe 29 et que recommande la CPVP aux termes de sa recommandation 06/2016, la CPVP attire ci-dessous l'attention des responsables de traitement et sous-traitants sur quelques-uns des éléments essentiels constitutifs de la fonction de délégué à la protection des données.

Quelles sont ses missions ?[18]

33. Dans l'accomplissement de ses missions, le délégué tient dûment compte du risque, pour les droits et libertés des personnes concernées, associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement. C'est l'approche basée sur les risques adoptée par le RGPD appliquée au travail du délégué à la protection des données.[19] Le considérant 75 explicite à cet égard :

> « Des risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie, peuvent résulter du traitement de données à caractère personnel qui est susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral, en particulier : (…) »

[17] Commission de la protection de la vie privée, Avis 33/2002 du 22 août 2002 portant sur le projet de loi relatif à la création du Centre fédéral d'expertise des soins de santé (point 21). Dans le même sens voy. Commission de la protection de la vie privée, Avis 19/2002 du 10 juin 2002 relatif aux (1) projet de loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, (2) projet d'arrêté royal relatif aux cartes d'identité et (3) projet d'arrêté royal portant mesures transitoire en ce qui concerne la carte d'identité électronique et Commission de la protection de la vie privée, Avis 23/2006 du 12 juillet 2006 portant sur l'avant-projet de loi relatif à l'encadrement des listes négatives (points 42 à 44).

[18] L'article 39 précise que les missions mentionnées doivent, au minimum, être confiées au délégué à la protection des données. Voy. pour plus de détails sur les missions du délégué à la protection des données le point 4. des Lignes directrices du Groupe 29 déjà citées.

[19] L'on retrouve cette approche basée sur les risques pour les personnes concernées dans la norme ISO 31000 et ISO 29134. Cette analyse des risques dépasse largement les risques de sécurité de l'information.

34. ***Contrôler le respect du règlement*** de manière générale: l'article 39.1.b) indique que la mission du délégué consiste à contrôler[20] le respect du règlement (c.à.d dans tous ses aspects, e.a. des principes relatifs aux traitements – finalité, licéité, proportionnalité etc. – aux droits des personnes concernées, aux obligations des responsables de traitement et sous-traitants ou encore l'encadrement des flux transfrontières ...), d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant.

    Le considérant 97 précise que le délégué à la protection des données devra aider le responsable du traitement et le sous-traitant à vérifier le respect, au niveau interne, du RGPD. Concrètement, il les assiste dans la mise en œuvre des éléments essentiels du règlement tels que les principes relatifs aux traitements des données (Chapitre II du RGPD), les droits des personnes concernées (Chapitre III du RGPD), la protection des données dès la conception et par défaut, le registre des activités de traitement, la sécurité du traitement, la notification et la communication des violations de données personnelles (data breach) etc. (art. 39.1. b) du RGPD).

    Dans ce cadre, le délégué peut, en particulier collecter des informations pour identifier les activités de traitement, analyser et vérifier la conformité des activités de traitement et informer, conseiller et émettre des recommandations. (Art. 39.1.a) du RGPD).[21] Globalement, la fonction de délégué devrait être davantage perçue comme une fonction d'accompagnement, de suivi (davantage reflétée par le terme anglais utilisé de « monitoring ») que de contrôle au sens strict du terme.

35. ***Rôle en matière d'analyse d'impact relative à la protection des données (art. 39.2.)*** : dans les conditions de l'article 35(1), il incombe au responsable de traitement - et non au délégué à la protection des données – d'effectuer une analyse d'impact relative à la protection des données (DPIA). Le délégué peut néanmoins jouer un rôle important en assistant le responsable de traitement à la demande de ce dernier (articles 35.2 et 39.1.c)). le responsable de traitement demandera conseil au délégué notamment sur les questions

[20] La version anglaise utilise le terme « monitor ».

[21] Voy. pour plus de détails sur ce volet des missions du délégué à la protection des données le point 4. 1. des Lignes directrices du Groupe 29 déjà cités.

suivantes : (1) effectuer ou non une analyse d'impact, (2) la méthode à utiliser pour effectuer l'analyse d'impact, (3) effectuer l'analyse d'impact en interne ou externaliser cette prestation, (4) les types de garanties à appliquer pour atténuer les risques pour les droits et libertés des personnes concernées et (5) l'évaluation en vue de déterminer si le DPIA a été correctement effectuée et si ses conclusions sont conformes au RGPD.[22]

36. ***Rôle du délégué dans la tenue du registre des activités de traitement*** : aux termes de l'article 30, il appartient au responsable de traitement et au sous-traitant – et non au délégué – de tenir « un registre des activités de traitement effectuées sous leur responsabilité » (art. 30.1. pour les responsables de traitement) ou « un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement » (art. 30.2. pour les sous-traitants). Le délégué à la protection des données doit être associé à ce travail de cartographie des traitements.

37. Le délégué est également tenu de **coopérer avec l'autorité de protection des données** (art. 39.1. d)) et de faire office de point de contact sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener des consultations, le cas échéant, sur tout autre sujet

38. Les missions confiées au délégué à la protection des données portent sur *tous* les aspects de la protection des données développés dans le RGPD en ce compris la sécurité des traitements dont le principe est énoncé, parmi d'autres, à l'article 5 § 1 f) et plus amplement détaillé à l'article 32 du RGPD.

39. Dans l'exercice de ses missions, le délégué doit être « facilement **joignable** au départ de chaque établissement (37.2. du RGPD). En d'autres termes, il doit être accessible[23].

40. Il doit par ailleurs être connu de l'autorité de contrôle à qui le responsable de traitement ou le sous-traitant doivent communiquer ses coordonnées (37.7. du RGPD)[24].

41. Il doit également être **connu des personnes concernées**, dont les employés de l'instance auprès de laquelle il exerce ses missions[25]. S'agissant de la comparaison avec le conseiller en sécurité, cette transparence s'ajoute à celle requise à l'article 4 de l'arrêté royal du 12 août 1993 déjà cité.

---

[22] Voy. pour plus de détails sur ce volet des missions du délégué à la protection des données le point 4.2 des Lignes directrices du Groupe 29 déjà cités.

[23] Voy. le point 2.3. des Lignes directrices du Groupe 29 sur le délégué à la protection des données.

[24] Voy. le point 2.5. des Lignes directrices du Groupe 29 sur le délégué à la protection des données.

[25] Idem.

42. Enfin, pour lui permettre d'exercer utilement sa fonction, le responsable de traitement ou le sous-traitant doivent veiller, au bénéfice du délégué:

- ***A l'associer en temps utile à toutes les questions relatives à la protection des données à caractère personnel*** : de manière générale, s'assurer que le délégué est informé et consulté dès le début facilitera la conformité avec le règlement et permettra notamment une approche réellement fondée sur la protection des données dès la conception (privacy by design) ;[26] Dans le même ordre d'idée, le conseiller en sécurité travaille en étroite collaboration avec les services qui le requièrent ou peuvent requérir son intervention.[27]

- ***A lui fournir des ressources suffisantes*** se traduisant par : un soutien actif de la direction, l'allocation de suffisamment de temps pour exercer ses missions, l'octroi de ressources financières, d'infrastructure et personnel le cas échéant suffisants, une communication officielle sur sa désignation en qualité de délégué à l'ensemble du personnel, un accès aux autres services ainsi qu'une formation continue. Selon la taille et la structure de l'organisme, il peut s'avérer nécessaire de constituer une équipe autour du délégué. La structure interne de l'équipe ainsi que les tâches et responsabilités de chacun devront être clairement établies[28]. S'agissant de la comparaison avec le conseiller en sécurité, la question de savoir s'il dispose du temps nécessaire relève de la compétence du Comité de surveillance ce qui ne sera pas le cas pour le délégué à la protection des données. Il appartiendra au seul responsable de traitement ou au sous-traitant d'évaluer si cette exigence est satisfaite. Le conseiller en sécurité doit tenir sa connaissance à jour ; s'agissant du délégué, le RGPD formule cette exigence sous la forme d'une obligation à charge du responsable de traitement et du sous-traitant.

- **A garantir son indépendance** (voy. infra le point 48) qui est entièrement consacré à cet aspect essentiel de la fonction).

Quel doit être son profil ? Une connaissance spécialisée du droit et des pratiques en matière de protection des données et une capacité à accomplir ses missions

43. Le RGPD indique que le délégué est désigné sur la base de ses qualités professionnelles, et en particulier de ses connaissances spécialisées du droit et des pratiques en matière de protection des données et de sa capacité à accomplir les missions visées à l'article 39 lesquelles dépassent la seule mise en œuvre d'une sécurité adéquate et les obligations relatives à

[26] Voy. le point 3.1. des Lignes directrices du Groupe 29 sur le délégué à la protection des données.

[27] Article 5 de l'arrêté royal du 12 août 1993 précité.

[28] Voy. le point 3.2. des Lignes directrices du Groupe 29 sur le délégué à la protection des données.

l'obligation de sécurité, par exemple la notification des violations de données (articles 33 et 34 du RGPD). Aucun diplôme défini ni certification particulière ne sont requis.

44. De manière générale, le niveau de connaissances spécialisées doit être déterminé en fonction des opérations de traitement de données effectuées et de la protection exigée pour les données traitées. Elle sera donc adaptée à la sensibilité, la complexité et le volume de données traitées, si les traitements impliquent des transferts réguliers ou occasionnels hors des frontières de l'Union etc. Outre un niveau d'expertise en protection des données, la connaissance du secteur d'activité et de l'organisation du responsable de traitement ou du sous-traitant est essentielle. Enfin, la capacité à accomplir ses missions doit s'entendre comme faisant référence à la fois aux qualités personnelles et aux connaissances du délégué mais également à sa position au sein de l'organisme. Ethique et intégrité sont liées au rôle clé qu'il doit jouer dans la promotion de la culture de la protection des données au sein de l'organisme, ce qui nécessitera souvent des capacités humaines de communication et de gestion des conflits. Comme déjà mentionné ci-dessus au point 42, aucun diplôme ni certification spécifique n'est requis aux termes du GDPR[29].

45. S'agissant du conseiller en sécurité, il incombe au Comité de surveillance[30] de vérifier qu'il dispose d'une connaissance suffisante pour mener sa mission bien. Comme cela a été mentionné au regard du temps nécessaire dont il doit disposer, il n'y a pas d'intervention prévue ni d'un Comité ni même de la Commission de la protection de la vie privée pour apprécier si oui ou non le délégué à la protection des données réunis les qualités requises. C'est un premier élément.

46. Deuxièmement, le RGPD va plus loin en exigeant que le délégué à la protection des données ait des connaissances spécialisées du droit et des pratiques en matière de protection des données ainsi qu'une capacité à accomplir les missions visées à l'article 39 lesquelles, comme mentionné ci-dessus au point 44, dépassent la seule mise en œuvre d'une sécurité adéquate et les obligations relatives à l'obligation de sécurité.

47. Le délégué n'en doit pas pour autant travailler seul. Il peut – et cela s'avérera le plus souvent souhaitable - s'appuyer sur les services et compétences existants, s'entourer d'une équipe aux profils multiples pour pouvoir au mieux réaliser ses missions ; l'exercice de celles-ci nécessitant une approche holistique de la protection des données et partant, une palette de compétences diverses et pointues. Dans ce cas, il est essentiel de prévoir une répartition claire des rôles de chacun et l'identification du délégué à la protection des données en tant que tel.

[29] Voy. le point 2.4. des Lignes directrices du Groupe 29 sur le délégué à la protection des données.

[30] Est ici visé le Comité de surveillance de la sécurité sociale et de la santé pour le conseiller en sécurité des institutions de sécurité sociale.

Quel doit être son statut ? Etre indépendant[31]

48. L'indépendance effective du délégué à la protection des données doit se traduire, aux termes du RGPD, de la façon suivante :

- Ne pas recevoir d'instructions en ce qui concerne l'exercice de ses missions (38.3. RGPD) : Le responsable de traitement ou le sous-traitant doivent s'assurer que le délégué ne reçoit aucune instruction en ce qui concerne l'exercice de ses missions. L'indépendance et l'autonomie du délégué dans l'exercice des missions qui sont les siennes ne signifie toutefois pas qu'il dispose de pouvoirs décisionnels allant au-delà de ses missions prévues à l'article 39 ;

- Ne pas être relevé de ses fonctions ou pénalisé pour l'exercice de ses misions (38.3. du RGPD) [32];

- Faire rapport directement au niveau le plus élevé de la direction (38.3. du RGPD) ;

- Etre soumis au secret professionnel ou à une obligation de confidentialité (38.5. du RGPD) : Cette obligation de secret professionnel ou de confidentialité[33] n'interdit toutefois pas au délégué de contacter ou de demander conseil à l'autorité de contrôle.

- Ne pas avoir de conflit d'intérêt (38.6. du RGPD) : à cet égard les lignes directrices du Groupe de l'article 29 mentionnent que les délégués peuvent exercer d'autres missions et tâches pour autant que celles-ci ne conduisent pas à un conflit d'intérêt. Cela implique notamment que le délégué ne peut occuper une fonction au sein de l'organisme qui le conduit à déterminer les finalités et les moyens des traitements[34]. En règle générale, les fonctions\positions conflictuelles au sein d'une entreprise peuvent comprendre des postes de direction (tels que directeur général, chef de l'exploitation, chef des finances, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du département informatique), mais peuvent également comprendre des fonctions établies plus bas dans la structure organisationnelle si ces postes ou fonctions permettent de déterminer les finalités ainsi que les moyens du traitement[35]. Le délégué à la protection des données a un rôle de conseil, d'accompagnement du responsable de traitement et du sous-traitant dans la mise en œuvre du RGPFD ainsi que de contrôle. Il

[31] Voy. le point 3.3. des Lignes directrices du Groupe 29 sur le délégué à la protection des données.

[32] Voy. le point 3.4. des Lignes directrices du Groupe 29 sur le délégué à la protection des données.

[33] La CPVP est d'avis que ce « secret professionnel » ne s'apparente pas au secret professionnel prévu à l'article 458 du Code pénal.

[34] La détermination des mesures de sécurité et leur mise en œuvre relèvent des moyens de traitement lesquels sont déterminés par le responsable de traitement.

[35] Voy. le point 3.5. des Lignes directrices du Groupe 29 sur le délégué à la protection des données.

ne peut donc être celui qui opère les traitements. Il est par contre celui qui conseille le responsable de traitement sur la manière dont ces traitements doivent être opérés. De la même manière qu'il est associé à la réalisation de l'analyse d'impact sans en supporter la responsabilité (laquelle incombe au responsable de traitement), il conseillera le responsable de traitement ou le sous-traitant en matière de sécurité sans lui-même mettre en œuvre les mesures nécessaires. S'il le faisait, il se trouverait dans une situation de conflit d'intérêt inadmissible au regard de sa fonction.

49. Sans mentionner le terme « indépendance », le conseiller en sécurité doit, comme déjà relevé, en application de l'arrêté royal du 12 août 1993, être placé sous l'autorité fonctionnelle directe du responsable de la gestion journalière. Il ne peut être relevé de sa fonction en raison des opinions qu'il émet ou des actes qu'il accomplit dans le cadre de l'exercice correct de sa fonction. Il ne peut non plus exercer d'activité qui pourraient être incompatibles.

Un certain nombre de garanties requises pour satisfaire à l'exigence d'indépendance du délégué à la protection des données existent aux termes de l'arrêt royal précité. C'est toutefois à l'aune de celles requises pour l'exercice de la fonction de délégué à la protection des données tel que prévues par le RGPD qu'il faudra les mettre en place.

V. CONCLUSION ET RECOMMANDATIONS

50. En conclusion des éléments de guidance explicités ci-dessus et dans les documents auxquels il est renvoyé pour plus de détails, la CPVP insiste sur les éléments ci-après :

- C'est à l'aune des exigences du RGPD au regard du délégué à la protection des données que doit se faire, par le responsable de traitement ou le sous-traitant concerné, l'examen de la question de savoir si un cumul de cette fonction avec une autre fonction ou une transition automatique d'une fonction à l'autre est admissible au regard du RGPD ;

- S'agissant des « conseillers en sécurité en particulier », il n'y a aucun automatisme ni transition systématique autorisée de cette fonction vers celle de délégué à la protection des données ; seul un examen *in concreto* par les responsables de traitement et sous-traitant concerné peut les guider à cet égard.

- La présente recommandation met en évidence que la mission du délégué à la protection des données porte sur toutes les dispositions du RGPD, soit sur tous les aspects de la protection des données personnelles (principes de licéité, finalité, proportionnalité et sécurité ; droits des personnes concernées ; protection des données dès la conception et par défaut ; registre des activités de traitement ; encadrement des flux transfrontières ; sécurité des traitements ; notification des violations de données (databreach)), y inclus tous les aspects de la sécurité des traitements et de l'information ;

- Le RGPD énonce une série d'éléments de garanties de l'indépendance du délégué à la protection des données (point 48) qu'il appartiendra aux responsables de traitements et sous-traitants de mettre en œuvre et à l'aune desquels, en fonction de l'organisation interne, la fonction de délégué à la protection des données devra être organisée;

- Enfin, s'agissant des qualifications du délégué, le RGPD exige que le délégué à la protection des données soit désigné sur la base de ses qualités professionnelles (en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données) et de sa capacité à accomplir ses missions. Ces missions couvrent comme rappelé ci-dessus, la protection des données dans *tous* ses aspects juridiques, techniques, organisationnels,…. La CPVP souligne l'importance de cette approche holistique de la protection des données et de la sécurité de l'information. Elle nécessitera le plus souvent que le délégué s'entoure de collaborateurs, de personnes ressources aux profils variés et expertise dans l'un ou l'autre aspect plus pointu. Qu'il travaille seul, en réseau, en équipe, le délégué à la protection des données devra toujours être clairement identifié. Ces qualifications et aptitude ne seront pas validées *a priori*, ni par la Commission de la protection de la vie privée, ni par un Comité sectoriel/ de surveillance si le concept de ces comités devait être conservé au terme de la réforme organique de la CPVP induite par le RGPD ;

- La CPVP recommande aux responsables de traitement et aux sous-traitants concernés de documenter leur choix ainsi que l'exercice de sa fonction par le délégué à la protection des données. Pour prouver la conformité au règlement, ils devraient constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape devront par ailleurs être réexaminés et actualisés régulièrement pour assurer une protection des données en continu ;

- Au titre de bonne pratique, la CPVP recommandé également que les responsables de traitement et sous-traitants identifient les postes incompatibles avec la fonction de délégué et élaborent des règles internes en vue d'éviter des conflits d'intérêt. Le rôle de *conseil* et de *contrôle (surveillance/monitoring)* de la mise en œuvre du RGPD par le délégué à la protection des données doit guider l'identification de ces conflits d'intérêt ;

- Enfin, la CPVP rappelle que le RGPD prévoit la possibilité de désigner un délégué externe dans le cadre de contrat de prestation de services.

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere