# Décision de la Commission nationale siégeant en formation restreinte sur l'issue de l'enquête n°[…] menée auprès de la « Fondation A »

Délibération n° 29FR/2021 du 4 août 2021

La Commission nationale pour la protection des données siégeant en formation restreinte, composée de Madame Tine A. Larsen, présidente, et de Messieurs Thierry Lallemang et Marc Lemmer, commissaires;

Vu le 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;

Vu la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, notamment son article 41;

Vu le règlement d'ordre intérieur de la Commission nationale pour la protection des données adopté par décision n°3AD/2020 en date du 22 janvier 2020, notamment son article 10, point 2;

Vu le règlement de la Commission nationale pour la protection des données relatif à la procédure d'enquête adopté par décision n°4AD/2020 en date du 22 janvier 2020, notamment son article 9;

Considérant ce qui suit :

## I. Faits et procédure

1. Vu l'impact du rôle du délégué à la protection des données (ci-après : le « DPD ») et l'importance de son intégration dans l'organisme, et considérant que les lignes directrices concernant les DPD sont disponibles depuis décembre 2016[1], soit 17 mois avant l'entrée en application du 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) (ci-après : le « RGPD »), la Commission nationale pour la protection des données (ci-après : la « Commission nationale » ou la « CNPD ») a décidé de lancer une campagne d'enquête thématique sur la fonction du DPD. Ainsi, 25 procédures d'audit ont été ouvertes en 2018, concernant tant le secteur privé que le secteur public.

2. En particulier, la Commission nationale a décidé par délibération n°[…] du 14 septembre 2018 d'ouvrir une enquête sous la forme d'audit sur la protection des données auprès de la « Fondation A » établie et ayant son siège au […], L-[…] et enregistrée au registre du commerce et des sociétés luxembourgeois sous le n°[…] (ci-après : le « contrôlé ») et de désigner M. Christophe Buschmann comme chef d'enquête. Ladite délibération précise que l'enquête porte sur la conformité du contrôlé avec la section 4 du chapitre 4 du RGPD.

3. Suivant l'article 2 de ses statuts, le contrôlé a pour objet [d'offrir des services sociaux].

4. Par courrier du 17 septembre 2018, le chef d'enquête a envoyé un questionnaire préliminaire au contrôlé auquel ce dernier a répondu par courrier du 5 octobre 2018. Une visite sur place a eu lieu le 13 février 2019. Suite à ces échanges, le chef d'enquête a établi le rapport d'audit n°[…] (ci-après : le « rapport d'audit »).

5. Il ressort du rapport d'audit qu'afin de vérifier la conformité de l'organisme avec la section 4 du chapitre 4 du RGPD, le chef d'enquête a défini onze objectifs de contrôle, à savoir :

1) S'assurer que l'organisme soumis à l'obligation de désigner un DPD l'a bien fait ;
2) S'assurer que l'organisme a publié les coordonnées de son DPD ;

[1] Les lignes directrices concernant les DPD ont été adoptées par le groupe de travail « Article 29 » le 13 décembre 2016. La version révisée (WP 243 rev. 01) a été adoptée le 5 avril 2017.

3) S'assurer que l'organisme a communiqué les coordonnées de son DPD à la CNPD ;
4) S'assurer que le DPD dispose d'une expertise et de compétences suffisantes pour s'acquitter efficacement de ses missions ;
5) S'assurer que les missions et les tâches du DPD n'entraînent pas de conflit d'intérêt ;
6) S'assurer que le DPD dispose de ressources suffisantes pour s'acquitter efficacement de ses missions ;
7) S'assurer que le DPD est en mesure d'exercer ses missions avec un degré suffisant d'autonomie au sein de son organisme ;
8) S'assurer que l'organisme a mis en place des mesures pour que le DPD soit associé à toutes les questions relatives à la protection des données ;
9) S'assurer que le DPD remplit sa mission d'information et de conseil auprès du responsable du traitement et des employés ;
10) S'assurer que le DPD exerce un contrôle adéquat du traitement des données au sein de son organisme ;
11) S'assurer que le DPD assiste le responsable du traitement dans la réalisation des analyses d'impact en cas de nouveaux traitements de données.

6. Par courrier du 18 octobre 2019 (ci-après : la « communication des griefs »), le chef d'enquête a informé le contrôlé des manquements aux obligations prévues par le RGPD qu'il a relevés lors de son enquête. Le rapport d'audit était joint audit courrier.

7. En particulier, le chef d'enquête a relevé dans la communication des griefs des manquements à

- l'obligation de désigner le DPD sur la base de ses qualités professionnelles[2] ;
- l'obligation de fournir les ressources nécessaires au DPD[3] ;
- l'obligation de garantir l'autonomie du DPD[4] ;
- l'obligation de veiller à ce que les autres missions et tâches du DPD n'entrainent pas de conflit d'intérêt[5] ;
- la mission de contrôle du DPD[6] ;
- la mission d'information et de conseil du DPD[7].

[2] Objectif n°4
[3] Objectif n°6
[4] Objectif n°7
[5] Objectif n°5
[6] Objectif n°10
[7] Objectif n°9

8. Par courrier du 14 novembre 2019, le contrôlé a adressé au chef d'enquête sa prise de position quant aux manquements relevés dans la communication des griefs.

9. Le 3 août 2020, le chef d'enquête a adressé au contrôlé un courrier complémentaire à la communication des griefs par lequel il informe le contrôlé sur les mesures correctrices et l'amende administrative qu'il propose à la Commission nationale siégeant en formation restreinte (ci-après : «la « formation restreinte ») d'adopter. Dans ce courrier, le chef d'enquête a proposé à la formation restreinte d'adopter cinq mesures correctrices différentes, ainsi que d'infliger au contrôlé une amende administrative d'un montant de 17.700 euros.

10. Par courrier du 19 août 2020, le contrôlé a fait parvenir au chef d'enquête ses observations quant au courrier complémentaire à la communication des griefs.

11. L'affaire a été à l'ordre du jour de la séance de la formation restreinte du 15 janvier 2021. Conformément à l'article 10.2. b) du règlement d'ordre intérieur de la Commission nationale, le chef d'enquête et le contrôlé ont présenté leurs observations orales à l'appui de leurs observations écrites et ont répondu aux questions posées par la formation restreinte. Le contrôlé a eu la parole en dernier.

## II. En droit

### A. Sur le manquement à l'obligation de désigner le DPD sur la base de ses qualités professionnelles

#### 1. Sur les principes

12. Selon l'article 37.5 du RGPD, « *[le DPD] 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 […]* ».

13. Aux termes du considérant (97) du RGPD, *« [l]e niveau de connaissances spécialisées requis devrait être déterminé notamment en fonction des opérations de traitement de données effectuées et de la protection exigée pour les données à caractère personnel traitées par le responsable du traitement ou le sous-traitant* ».

14. Par ailleurs, le groupe de travail « Article 29 » sur la protection des données a adopté le 13 décembre 2016 des lignes directrices concernant les DPD qui ont été reprises et réapprouvées par le comité européen de la protection des données en date du 25 mai 2018[8]. Ces lignes directrices précisent que le niveau d'expertise du DPD « *doit être proportionné à la sensibilité, à la complexité et au volume des données traitées par un organisme* »[9] et qu'« *il est nécessaire que les DPD disposent d'une expertise dans le domaine des législations et pratiques nationales et européennes en matière de protection des données, ainsi que d'une connaissance approfondie du RGPD* »[10].

15. Les lignes directrices concernant les DPD indiquent ensuite que « [l]*a connaissance du secteur d'activité et de l'organisme du responsable du traitement est utile. Le DPD devrait également disposer d'une bonne compréhension des opérations de traitement effectuées, ainsi que des systèmes d'information et des besoins du responsable du traitement en matière de protection et de sécurité des données* »[11].

2. <u>En l'espèce</u>

16. Il résulte du rapport d'audit que, pour que le chef d'enquête considère l'objectif 4 comme rempli par le contrôlé dans le cadre de cette campagne d'audit, il s'attend à ce que le DPD ait au minimum trois ans d'expérience professionnelle en matière de protection des données.

17. Selon la communication des griefs, page 3, il a été constaté lors de l'enquête que le DPD « *dispose de moins de 3 ans d'expérience professionnelle en matière de protection des données »* et qu'il *« ne dispose pas lui-même d'expertise juridique.* ». Le chef d'enquête précise aussi que le DPD a accès à un cabinet d'avocats en cas de besoin, mais que « *cet accès est conditionné à l'approbation de la hiérarchie du DPD* ». Le chef d'enquête en conclut qu'il *« existe dès lors un risque que le DPD ne puisse pas accéder à l'expertise juridique dont il a pourtant besoin. »*

18. Dans sa prise de position du 14 novembre 2019, le contrôlé indique avoir pris « *la décision d'engager un nouveau DPD disposant de compétences élargies (compétences*

[8] WP 243 v.01, version révisée et adoptée le 5 avril 2017
[9] WP 243 v.01, version révisée et adoptée le 5 avril 2017, p. 13
[10] WP 243 v.01, version révisée et adoptée le 5 avril 2017, p. 14
[11] WP 243 v.01, version révisée et adoptée le 5 avril 2017, p.14

*juridiques; compétences techniques) ainsi qu'une expérience confirmée et un cursus professionnel plus en ligne avec le rôle de DPD* ». Le contrôlé précise que le nouveau DPD, dont le CV a été communiqué en annexe à sa prise de position du 14 novembre 2019, a été engagé et nommé en date du 13 novembre 2019.

19. La formation restreinte relève d'abord que dans sa prise de position du 14 novembre 2019, le contrôlé ne met pas en cause les constatations faites par le chef d'enquête quant à l'expérience professionnelle en matière de protection des données du DPD qui était en fonction au moment de l'ouverture de l'enquête. Elle relève aussi qu'il n'est pas non plus contesté par le contrôlé que le DPD pouvait rencontrer des difficultés pour accéder à l'expertise juridique dont il avait pourtant besoin, l'accès au support juridique externe étant conditionné à l'approbation de la hiérarchie du DPD.

20. La formation restreinte relève ensuite qu'il est précisé à juste titre en page 2 de la communication des griefs (sous « remarques préliminaires ») que « [l]*es exigences du RGPD ne sont pas toujours strictement définies. Dans une telle situation, il revient aux autorités de contrôle de vérifier la proportionnalité des mesures mises en place par les responsables de traitement au regard de la sensibilité des données traitées et des risques encourus par les personnes concernées*. »

21. Or, la formation restreinte constate qu'il est aussi précisé en page 2 de la communication des griefs, que le contrôlé « *[…]* », que l'activité de […] et que le contrôlé « *emploie environ […] collaborateurs* ». Le chef d'enquête en conclut que le contrôlé traite un nombre substantiel de données dont le degré de sensibilité peut être relativement élevé, tels que des données médicales. La formation restreinte partage cette appréciation et considère dès lors que le niveau d'expertise du DPD qui était en fonction au moment de l'ouverture de l'enquête n'était pas suffisant au regard de la sensibilité des données traitées.

22. La formation restreinte prend note du fait qu'un nouveau DPD, disposant d'une expertise suffisante en matière de protection des données, et dont le CV a été communiqué par le contrôlé avec sa prise de position du 14 novembre 2019, a été désigné en cours d'enquête. Si une telle mesure devrait permettre au contrôlé de se mettre en conformité, il convient néanmoins de constater que celle-ci a été décidée en cours d'enquête. La formation restreinte se rallie par conséquent au constat du chef d'enquête selon lequel, au début de

l'enquête, le contrôlé n'a pas été en mesure de démontrer qu'il a désigné un DPD avec les qualités professionnelles suffisantes.

23. Au vu de ce qui précède, la formation restreinte conclut que l'article 37.5 du RGPD n'a pas été respecté par le contrôlé.

B. Sur le manquement à l'obligation de fournir les ressources nécessaires au DPD

1. Sur les principes

24. L'article 38.2 du RGPD exige que l'organisme aide son DPD *« à exercer les missions visées à l'article 39 en fournissant les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et lui permettant d'entretenir ses connaissances spécialisées.* »

25. Il résulte des lignes directrices concernant les DPD que les aspects suivants doivent notamment être pris en considération[12] :

- « *temps suffisant pour que les DPD puissent accomplir leurs tâches. Cet aspect est particulièrement important lorsqu'un DPD interne est désigné à temps partiel ou lorsque le DPD externe est chargé de la protection des données en plus d'autres tâches. Autrement, des conflits de priorités pourraient conduire à ce que les tâches du DPD soient négligées. Il est primordial que le DPD puisse consacrer suffisamment de temps à ses missions. Il est de bonne pratique de fixer un pourcentage de temps consacré à la fonction de DPD lorsque cette fonction n'est pas occupée à temps plein. Il est également de bonne pratique de déterminer le temps nécessaire à l'exécution de la fonction et le niveau de priorité approprié pour les tâches du DPD, et que le DPD (ou l'organisme) établisse un plan de travail* ;
- *accès nécessaire à d'autres services, tels que les ressources humaines, le service juridique, l'informatique, la sécurité, etc., de manière à ce que les DPD puissent recevoir le soutien, les contributions et les informations essentiels de ces autres services* ».

26. Les lignes directrices concernant les DPD précisent que « [d]*'une manière générale, plus les opérations de traitement sont complexes ou sensibles, plus les ressources octroyées*

[12] WP 243 v.01, version révisée et adoptée le 5 avril 2017, p. 17

*au DPD devront être importantes. La fonction de protection des données doit être effective et dotée de ressources adéquates au regard du traitement de données réalisé.* »

2. <u>En l'espèce</u>

27. Il ressort du rapport d'audit qu'au vu de la taille des organismes sélectionnés dans le cadre de cette campagne d'audit, pour que le chef d'enquête considère l'objectif 6 comme rempli par le contrôlé, il s'attend à ce que le contrôlé ait au minimum un ETP (équivalent temps plein) pour l'équipe en charge de la protection des données. Le chef d'enquête s'attend également à ce que le DPD ait la possibilité de s'appuyer sur d'autres services, tels que le service juridique, l'informatique, la sécurité, etc.

28. D'après le rapport d'audit, le DPD exerce sa fonction « *à hauteur de 0.5 ETP* ». Il est par ailleurs précisé que le DPD dispose « *de l'appui d'un prestataire externe, spécialisé en matière de protection des données* ».

29. Dans la communication des griefs, page 3, le chef d'enquête précise que « *Compte tenu de l'existence d'opérations de traitement complexes ou sensibles (voir remarques préliminaires), il est attendu un niveau élevé de ressources.* ». Or, le chef d'enquête relève que « *le DPD est affecté à 50%* », qu'il « *exerce seul ses missions* » et que le fait qu'il « *bénéficie de l'appui d'un prestataire externe, spécialisé en matière de protection des données, ne saurait suffire à fournir un temps suffisant pour que le DPD accomplisse ses missions.* »

30. Dans sa prise de position du 14 novembre 2019, le contrôlé indique que le DPD nouvellement désigné « *est affecté à temps complet aux diverses missions qui lui incombent en tant que DPD* ». Le contrôlé indique aussi que le DPD « *assiste toutefois aussi le […] dans ses missions de contrôle et d'audit.* » Enfin, le contrôlé précise que le DPD a la possibilité de recourir à une « *expertise juridique externe* » ainsi qu'à des « *prestataires externes spécialisés en matière de protection des données* ».

31. Néanmoins, dans sa réponse du 19 août 2020 au courrier complémentaire, le contrôlé apporte des précisions quant au temps consacré par le DPD à l'exercice de ses missions et indique en particulier qu'il « *effectue sa mission de DPO sur une période de 80 % de son temps. Les 20 % restants consistent à assister la […] dans la gestion contractuelle avec les intervenants externes.* »

32. Il convient d'abord de relever que la formation restreinte partage l'appréciation du chef d'enquête formulée en page 3 de la communication des griefs selon laquelle « *Compte tenu de l'existence d'opérations de traitement complexes ou sensibles (voir remarques préliminaires), il est attendu un niveau élevé de ressources. ».* Or, il a été constaté au début de l'enquête que le DPD ne consacrait que 50% de son temps de travail à l'exercice de ses missions. L'indication selon laquelle le DPD disposait du support d'un prestataire externe ne constitue pas un élément suffisant pour démontrer que le DPD disposait des ressources suffisantes pour s'acquitter de ses missions. La formation restreinte se rallie par conséquent au constat du chef d'enquête selon lequel le responsable du traitement n'a pas été en mesure de démontrer qu'il a fourni les ressources nécessaires au DPD pour l'exercice de ses missions.

33. Enfin, si la formation restreinte a pu vérifier qu'un nouveau DPD a effectivement été désigné par le contrôlé en cours d'enquête, elle ne dispose pas néanmoins de la documentation qui permettrait de vérifier qu'il dispose de ressources suffisantes, et relève en particulier que dans sa réponse du 19 août 2020 au courrier complémentaire, le contrôlé a indiqué que le DPD exerce ses missions à 80%.

34. Au vu de ce qui précède, la formation restreinte conclut que l'article 38.2 du RGPD n'a pas été respecté par le contrôlé.

C. Sur le manquement à l'obligation de garantir l'autonomie du DPD

1. Sur les principes

35. Aux termes de l'article 38.3 du RGPD, l'organisme doit veiller à ce que le DPD « *ne reçoive aucune instruction en ce qui concerne l'exercice des missions* ». Par ailleurs, le DPD « *fait directement rapport au niveau le plus élevé de la direction »* de l'organisme.

36. Le considérant (97) du RGPD indique en outre que les DPD « *devraient être en mesure d'exercer leurs fonctions et missions en toute indépendance* ».

37. Selon les lignes directrices concernant les DPD[13], l'article 38.3 du RGPD « *prévoit certaines garanties de base destinées à faire en sorte que les DPD soient en mesure d'exercer leurs missions avec un degré suffisant d'autonomie au sein de leur organisme. […] Cela signifie que, dans l'exercice de leurs missions au titre de l'article 39, les DPD ne doivent pas recevoir d'instructions sur la façon de traiter une affaire, par exemple, quel résultat devrait être*

[13] WP 243 v.01, version révisée et adoptée le 5 avril 2017, p. 17 et 18

*obtenu, comment enquêter sur une plainte ou s'il y a lieu de consulter l'autorité de contrôle. En outre, ils ne peuvent être tenus d'adopter un certain point de vue sur une question liée à la législation en matière de protection des données, par exemple, une interprétation particulière du droit. […] Si le responsable du traitement ou le sous-traitant prend des décisions qui sont incompatibles avec le RGPD et l'avis du DPD, ce dernier devrait avoir la possibilité d'indiquer clairement son avis divergent au niveau le plus élevé de la direction et aux décideurs. À cet égard, l'article 38, paragraphe 3, dispose que le DPD « fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant ». Une telle reddition de compte directe garantit que l'encadrement supérieur (par ex., le conseil d'administration) a connaissance des avis et recommandations du DPD qui s'inscrivent dans le cadre de la mission de ce dernier consistant à informer et à conseiller le responsable du traitement ou le sous-traitant. L'élaboration d'un rapport annuel sur les activités du DPD destiné au niveau le plus élevé de la direction constitue un autre exemple de reddition de compte directe.* »

2. <u>En l'espèce</u>

38. Il ressort du rapport d'audit que, pour que le chef d'enquête considère l'objectif 7 comme rempli par le contrôlé dans le cadre de cette campagne d'audit, il s'attend à ce que le DPD soit « *rattaché au plus haut niveau de la direction afin de garantir au maximum son autonomie* ».

39. Selon la communication des griefs, page 4, « [i]*l ressort de l'enquête que le DPD est rattaché au Directeur […]. Bien que formellement, dans la déclaration de nomination, il soit prévu que le DPD rende compte directement au comité de direction une fois par trimestre, dans les faits, la remontée d'information se fait uniquement par l'intermédiaire du Directeur de rattachement.* »

40. Dans sa prise de position du 14 novembre 2019, le contrôlé fait valoir que le DPD nouvellement désigné est « *totalement autonome et rend compte directement au niveau le plus élevé de la direction. Il assiste au Comité de Direction et aux diverses réunions […].* » Le contrôlé précise en outre que « [d]*es entrevues régulières sont planifiées avec les membres de la Direction […]* (…) » et que « [d]*es entrevues récurrentes sur base trimestrielle sont planifiées de manière fixe à la gouvernance du Comité de direction (planning annuel). »*

41. S'il ne résulte pas des dispositions du RGPD que le DPD doit nécessairement être rattaché au niveau le plus élevé de la direction afin de garantir son autonomie, la formation restreinte rappelle néanmoins qu'elle a relevé au point 20 de la présente décision qu'il est

précisé à juste titre en page 2 de la communication des griefs (sous « remarques préliminaires ») que « [l]*es exigences du RGPD ne sont pas toujours strictement définies. Dans une telle situation, il revient aux autorités de contrôle de vérifier la proportionnalité des mesures mises en place par les responsables de traitement au regard de la sensibilité des données traitées et des risques encourus par les personnes concernées.* »

42. Or, tel que cela est mentionné au point 21 de la présente décision, la formation restreinte partage l'appréciation du chef d'enquête, mentionnée en page 2 de la communication des griefs, selon laquelle le contrôlé traite un nombre substantiel de données dont le degré de sensibilité peut être relativement élevé, tels que des données médicales. La formation restreinte considère dès lors que, en l'absence d'autres mesures qui permettraient de démontrer que le DPD est en mesure d'accéder directement au plus haut niveau de la direction dès qu'il l'estime nécessaire, le rattachement hiérarchique du DPD au plus haut niveau de la direction, suivant l'attente du chef d'enquête, constitue une mesure proportionnée afin de garantir son autonomie. A cet égard, la formation restreinte constate qu'au début de l'enquête, le DPD du contrôlé était rattaché au directeur […] et non au plus haut niveau de la direction. Elle constate aussi que le contrôlé ne met pas en cause la précision apportée par le chef d'enquête dans la communication des griefs selon laquelle bien qu'« *il soit prévu que le DPD rende compte directement au comité de direction une fois par trimestre, dans les faits, la remontée d'information se fait uniquement par l'intermédiaire du Directeur de rattachement.* »

43. La formation restreinte se rallie par conséquent au constat du chef d'enquête selon lequel, au début de l'enquête, le responsable de traitement n'a pas été en mesure de démontrer que le DPD faisait directement rapport au niveau le plus élevé de la direction.

44. Au vu de ce qui précède, la formation restreinte conclut que l'article 38.3 du RGPD n'a pas été respecté par le contrôlé.

D. <u>Sur le manquement relatif à l'obligation de veiller à ce que les autres missions et tâches du DPD n'entrainent pas de conflit d'intérêts</u>

1. <u>Sur les principes</u>

45. Selon l'article 38.6 du RGPD, « [le DPD] *peut exécuter d'autres missions et tâches. Le responsable du traitement ou le sous-traitant veille à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts* ».

46. Les lignes directrices concernant les DPD[14] précisent que « *le DPD ne peut exercer au sein de l'organisme une fonction qui l'amène à déterminer les finalités et les moyens du traitement de données à caractère personnel* ». Selon les lignes directrices, « [e]*n règle générale, parmi les fonctions susceptibles de donner lieu à un conflit d'intérêts au sein de l'organisme peuvent figurer les fonctions d'encadrement supérieur (par exemple : directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du service informatique), mais aussi d'autres rôles à un niveau inférieur de la structure organisationnelle si ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement. En outre, il peut également y avoir conflit d'intérêts, par exemple, si un DPD externe est appelé à représenter le responsable du traitement ou le sous-traitant devant les tribunaux dans des affaires ayant trait à des questions liées à la protection des données.*

*En fonction des activités, de la taille et de la structure de l'organisme, il peut être de bonne pratique pour les responsables du traitement ou les sous-traitants :*

- *de recenser les fonctions qui seraient incompatibles avec celle de DPD ;*
- *d'établir des règles internes à cet effet, afin d'éviter les conflits d'intérêts ;*
- *d'inclure une explication plus générale concernant les conflits d'intérêts ;*
- *de déclarer que le DPD n'a pas de conflit d'intérêts en ce qui concerne sa fonction de DPD, dans le but de mieux faire connaître cette exigence ;*
- *de prévoir des garanties dans le règlement intérieur de l'organisme, et de veiller à ce que l'avis de vacance pour la fonction de DPD ou le contrat de service soit suffisamment précis et détaillé pour éviter tout conflit d'intérêts. Dans ce contexte, il convient également de garder à l'esprit que les conflits d'intérêts peuvent prendre différentes formes selon que le DPD est recruté en interne ou à l'extérieur.* »

2. <u>En l'espèce</u>

47. Il résulte du rapport d'audit que, pour que le chef d'enquête considère l'objectif 5 comme atteint par le contrôlé dans le cadre de cette campagne d'audit, il s'attend à ce que, dans le cas où le DPD exerce d'autres fonctions au sein de l'organisme contrôlé, ces fonctions n'entraînent pas de conflit d'intérêts notamment par l'exercice de fonctions qui amènerait le DPD à déterminer les finalités et les moyens du traitement de données à caractère personnel.

[14] WP 243 v.01, version révisée et adoptée le 5 avril 2017, pp.19-20

Le chef d'enquête s'attend également à ce que le contrôlé ait réalisé une analyse quant à l'existence d'un éventuel conflit d'intérêts au niveau du DPD.

48. D'après la communication des griefs, page 4, « [i]*l ressort de l'enquête qu'avant d'être nommé DPD, ce dernier était responsable du service IT. Il exerce par ailleurs, parallèlement à ses missions de DPD, la fonction de […]. Si dans le cadre de ses missions de […], le DPD ne participe pas à […], il n'en reste pas moins que ce dernier était impliqué dans la mise en place de traitements de données à caractère personnel dans le cadre de ses fonctions de responsable de service IT. Le DPD pourrait donc être amené à se prononcer sur des traitements qu'il a lui-même mis en place en tant que responsable du service IT.* » Le chef d'enquête précise en outre que le contrôlé *« n'a pas su apporter d'élément, tel que la nomination d'un DPD ad hoc pour analyser les traitements informatiques, permettant d'adresser le risque de conflit d'intérêt.* »

49. Dans sa prise de position du 14 novembre 2019, sans mettre en cause les constatations faites par le chef d'enquête dans la communication des griefs, le contrôlé indique que « [p]*ar la nomination d'un nouveau DPD à tâche complète, il est garanti qu'il n'y ait pas de conflits d'intérêts* » et précise que ce nouveau DPD « *n'exerce aucune autre fonction* ».

50. La formation restreinte constate que la désignation d'un nouveau DPD qui n'exercerait aucune autre fonction auprès du contrôlé, si ce n'est une fonction de support auprès de la […] pour la « *gestion contractuelle des intervenants externes* » (d'après la réponse du contrôlé du 19 août 2020 au courrier complémentaire), permettrait d'assurer que le DPD du contrôlé ne serait pas amené à se prononcer sur des traitements dont il aurait contribué à déterminer les finalités et les moyens.

51. Néanmoins, la formation restreinte relève que la désignation du nouveau DPD est intervenue en cours d'enquête et se rallie par conséquent au constat du chef d'enquête, selon lequel, au début de l'enquête, le contrôlé n'a pas su démontrer qu'il n'existait pas de conflit d'intérêt résultant des fonctions antérieures exercées par le DPD qui était alors en fonction.

52. Au vu de ce qui précède, la formation restreinte conclut que l'article 38.6 du RGPD n'a pas été respecté par le contrôlé.

E. Sur le manquement relatif à la mission d'information et de conseil du DPD

1. Sur les principes

53. En vertu de l'article 39.1.a) du RGPD, l'une des missions du DPD est d'*« informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du présent règlement et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données* ».

2. En l'espèce

54. Il ressort du rapport d'audit que, pour que le chef d'enquête considère l'objectif 9 comme rempli par le contrôlé dans le cadre de cette campagne d'audit, le chef d'enquête s'attend à ce que « *l'organisme dispose d'un reporting formel des activités du DPD vers le Comité de Direction sur base d'une fréquence définie. Concernant l'information aux employés, il est attendu que l'organisme ait mis en place un dispositif de formation adéquat du personnel en matière de protection des données* ».

55. Sur ces deux points, selon la communication des griefs, page 5, « [i]*l ressort de l'enquête qu'[…], les chefs de service ainsi que les membres de la direction ont été sensibilisés à la protection des données personnelles. Les […] agissent ensuite en tant que relais de la sensibilisation vers les autres membres du personnel. Une sensibilisation a également été faite auprès du conseil d'administration et du […]. En revanche, à la date de la visite des agents de la CNPD, le DPD n'avait participé à aucun comité de direction et sa participation n'était pas prévue, le reporting vers le comité de direction se faisant via le directeur […]. Par ailleurs, il n'existe pas d'outil tel qu'un rapport d'activité qui aurait pu permettre au DPD d'adresser des conseils formels au responsable de traitement. »*

56. La formation restreinte constate que le manquement relevé par le chef d'enquête ne concerne que la mission d'information et de conseil du DPD à l'égard du responsable du traitement, et non pas la mission d'information et de conseil du DPD à l'égard des employés. La formation restreinte prend néanmoins note des mesures qui ont été décidées par le contrôlé pour renforcer la sensibilisation de ses collaborateurs, lesquelles sont décrites dans sa prise de position du 14 novembre 2019.

57. Pour ce qui est de la mission d'information et de conseil à l'égard du responsable du traitement, dans sa prise de position du 14 novembre 2019, le contrôlé indique que « *Toutes*

*réunions et actions (information, sensibilisation, conseil, contrôle, audit, etc.) seront documentées en vue d'un rapport d'activités à l'attention de la Direction […] et à qui de droit.* »

58. La formation restreinte relève que l'article 39.1 du RGPD énumère les missions que le DPD doit au moins se voir confier, dont la mission d'informer et de conseiller l'organisme ainsi que les employés, sans toutefois préciser si des mesures spécifiques doivent être mise en place pour assurer que le DPD puisse accomplir sa mission d'information et de conseil. Les lignes directrices concernant les DPD, qui formulent des recommandations et des bonnes pratiques pour guider les responsables de traitement dans la mise en conformité à l'égard de leur gouvernance, n'abordent également que succinctement la mission de conseil et d'information du DPD. Ainsi, elles précisent que la tenue du registre des activités de traitement visé à l'article 30 du RGPD peut être confiée au DPD et que « *[c]e registre doit être considéré comme l'un des outils permettant au DPD d'exercer ses missions de contrôle du respect du RGPD ainsi que d'information et de conseil du responsable du traitement ou du sous-traitant*.[15] »

59. A cet égard, il ressort du dossier d'enquête que le DPD en fonction au moment de l'ouverture de l'enquête utilisait le registre afin de vérifier que la documentation nécessaire existait pour chaque traitement ainsi que pour identifier les traitements devant faire l'objet d'une analyse d'impact[16].

60. Néanmoins, la formation restreinte rappelle qu'elle a déjà constaté au point 20 de la présente décision qu'il est précisé à juste titre en page 2 de la communication des griefs (sous « remarques préliminaires ») que « [l]*es exigences du RGPD ne sont pas toujours strictement définies. Dans une telle situation, il revient aux autorités de contrôle de vérifier la proportionnalité des mesures mises en place par les responsables de traitement au regard de la sensibilité des données traitées et des risques encourus par les personnes concernées. »*

61. Or, tel que cela est mentionné au point 21 de la présente décision, la formation restreinte partage l'appréciation du chef d'enquête, mentionnée en page 2 de la communication des griefs, selon laquelle le contrôlé traite un nombre substantiel de données dont le degré de sensibilité peut être relativement élevé, tels que des données médicales. La formation restreinte considère dès lors qu'un reporting formel des activités du DPD auprès de la direction, sur la base d'une fréquence définie, constitue une mesure proportionnée afin de

[15] WP 243 v.01, version révisée et adoptée le 5 avril 2017, p. 22

[16] Compte-rendu de la visite du 13 février 2019, points 8 et 11

démontrer que le DPD exerce ses missions d'information et de conseil à l'égard du responsable du traitement.

62. La formation restreinte prend note des mesures qui ont été décidées en ce sens par le contrôlé, lesquelles sont décrites dans sa prise de position du 14 novembre 2019. Néanmoins, la formation restreinte constate d'une part, que la fréquence à laquelle les rapports d'activités sont adressés à la Direction […] n'a pas été explicitée et d'autre part, que ces mesures ont été décidées en cours d'enquête. Elle se rallie par conséquent au constat du chef d'enquête selon lequel, au début de l'enquête, le responsable de traitement n'a pas été en mesure de démontrer que le DPD exerce ses missions d'information et de conseil à l'égard du responsable de traitement.

63. La formation restreinte constate en outre qu'elle ne dispose pas de la documentation qui lui permettrait de vérifier la mise en œuvre des mesures décidées par le contrôlé.

64. Au vu de ce qui précède, la formation restreinte conclut que l'article 39.1. a) du RGPD n'a pas été respecté par le contrôlé.

F. Sur le manquement relatif à la mission de contrôle du DPD

1. Sur les principes

65. Selon l'article 39.1. b) du RGPD, le DPD a, entre autres, la mission de « *contrôler le respect du présent règlement, 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 DPD devrait aider l'organisme à vérifier le respect, au niveau interne, du RGPD.

66. Il résulte des lignes directrices concernant les DPD[17] que le DPD peut, dans le cadre de ces tâches de contrôle, notamment :

- recueillir des informations permettant de recenser les activités de traitement;
- analyser et vérifier la conformité des activités de traitement;

[17] WP 243 v.01, version révisée et adoptée le 5 avril 2017, p. 20

- informer et conseiller le responsable du traitement ou le sous-traitant et formuler des recommandations à son intention.

2. <u>En l'espèce</u>

67. Il ressort du rapport d'audit que, pour qu'il puisse considérer l'objectif 10 comme rempli par le contrôlé dans le cadre de cette campagne d'audit, le chef d'enquête s'attend à ce que « *l'organisme dispose d'un plan de contrôle formalisé en matière de protection des données (même s'il n'est pas encore exécuté)* ».

68. Selon la communication des griefs, p. 5, *«* [i]*l ressort de l'enquête que l'organisme ne dispose pas d'un plan de contrôle formalisé mais d'une liste de tâches, comprenant des points de contrôle. Dans une logique de gestion quotidienne de la protection des données, et compte-tenu du nombre de données traitées et de leur sensibilité (voir les remarques préliminaires), il est attendu que les missions de contrôle du DPD* (…) *soient mieux formalisées.* »

69. Dans sa prise de position du 14 novembre 2019, le contrôlé indique que le nouveau DPD a développé et mis en œuvre un « *[…] dédié au RGPD* » qui « *comprend le registre des traitements et divers points de contrôle avec date de révision de ces derniers* ». Le contrôlé précise que « [l]*es analyses DPIA effectuées sur base de […] sont directement jointes aux divers traitements. Ces diverses actions sont enregistrées dans un calendrier faisant partie intégrante de ce logiciel.* »

70. La formation restreinte constate que l'article 39.1 du RGPD énumère les missions que le DPD doit au moins se voir confier, dont la mission de contrôler le respect du RGPD, sans toutefois exiger que l'organisme mette en place des mesures spécifiques pour assurer que le DPD puisse accomplir sa mission de contrôle. Les lignes directrices concernant les DPD indiquent notamment que la tenue du registre des activités de traitement visé à l'article 30 du RGPD peut être confiée au DPD et que « *[c]e registre doit être considéré comme l'un des outils permettant au DPD d'exercer ses missions de contrôle du respect, du RGPD ainsi que d'information et de conseil du responsable du traitement ou du sous-traitant*.[18] »

71. La formation restreinte a déjà relevé au point 59 de la présente décision qu'il ressort du dossier d'enquête que le DPD en fonction au moment de l'ouverture de l'enquête utilisait le

[18] WP 243 v.01, version révisée et adoptée le 5 avril 2017, p. 22

registre afin de vérifier que la documentation nécessaire existait pour chaque traitement ainsi que pour identifier les traitements devant faire l'objet d'une analyse d'impact[19]. La formation restreinte relève néanmoins que ces éléments pris isolément ne sont pas suffisants pour permettre au contrôlé de démontrer que le DPD puisse effectuer sa mission de contrôle du respect du RGPD de manière adéquate.

72. La formation restreinte rappelle qu'elle a relevé au point 20 de la présente décision qu'il est précisé à juste titre en page 2 de la communication des griefs (sous « remarques préliminaires ») que « [l]*es exigences du RGPD ne sont pas toujours strictement définies. Dans une telle situation, il revient aux autorités de contrôle de vérifier la proportionnalité des mesures mises en place par les responsables de traitement au regard de la sensibilité des données traitées et des risques encourus par les personnes concernées.* »

73. Or, tel que cela est mentionné au point 21 de la présente décision, la formation restreinte partage l'appréciation du chef d'enquête, mentionnée en page 2 de la communication des griefs, selon laquelle le contrôlé traite un nombre substantiel de données dont le degré de sensibilité peut être relativement élevé, tels que des données médicales.

74. La formation restreinte considère par conséquent que la mission de contrôle effectuée par le DPD auprès du contrôlé devrait être suffisamment formalisée, par exemple par un plan de contrôle en matière de protection des données, afin de permettre au contrôlé de démontrer que le DPD puisse effectuer sa mission de contrôle du respect du RGPD de manière adéquate.

75. Or, la formation restreinte constate qu'il ressort du dossier d'enquête et des éléments communiqués par le contrôlé dans sa prise de position du 14 novembre 2019 que la mission de contrôlé effectuée par le DPD n'était pas suffisamment formalisée au moment de l'ouverture de l'enquête.

76. La formation restreinte prend note du fait que dans son courrier du 19 août 2020, le contrôlé indique que le nouveau DPD « *a déjà fait modifier différentes procédures internes afin que la protection des données à caractère personnel soit bien prise en compte au sein de nos diverses activités* » et qu'un *« plan de suivi de nos divers traitements, en fonction de leurs sensibilités, a* (…) *été mis en place. »*

77. Néanmoins, la formation restreinte constate que ces mesures ont été décidées en cours d'enquête et se rallie par conséquent au constat du chef d'enquête selon lequel, au

[19] Compte-rendu de la visite du 13 février 2019, points 8 et 11

début de l'enquête, le contrôlé n'a pas été en mesure de démontrer que le DPD exerce ses missions de contrôle du respect du RGPD de manière adaptée à ses besoins.

78. La formation restreinte constate en outre qu'elle ne dispose pas de la documentation qui permettrait de démontrer que les mesures mentionnées au point 76 de la présente décision ont été mises en place par le contrôlé.

79. Au vu de ce qui précède, la formation restreinte conclut que l'article 39.1. b) du RGPD n'a pas été respecté par le contrôlé.

## III. Sur les mesures correctrices et l'amende

### A. Les principes

80. Conformément à l'article 12 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale dispose des pouvoirs prévus à l'article 58.2 du RGPD :

*a) avertir un responsable du traitement ou un sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions du présent règlement;*

*b) rappeler à l'ordre un responsable du traitement ou un sous-traitant lorsque les opérations de traitement ont entraîné une violation des dispositions du présent règlement;*

*c) ordonner au responsable du traitement ou au sous-traitant de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits en application du présent règlement;*

*d) ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec les dispositions du présent règlement, le cas échéant, de manière spécifique et dans un délai déterminé;*

*e) ordonner au responsable du traitement de communiquer à la personne concernée une violation de données à caractère personnel;*

*f) imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement;*

*g) ordonner la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement en application des articles 16, 17 et 18 et la notification de ces mesures aux destinataires auxquels les données à caractère personnel ont été divulguées en application de l'article 17, paragraphe 2, et de l'article 19;*

*h) retirer une certification ou ordonner à l'organisme de certification de retirer une certification délivrée en application des articles 42 et 43, ou ordonner à l'organisme de certification de ne pas délivrer de certification si les exigences applicables à la certification ne sont pas ou plus satisfaites;*

*i) imposer une amende administrative en application de l'article 83, en complément ou à la place des mesures visées au présent paragraphe, en fonction des caractéristiques propres à chaque cas;*

*j) ordonner la suspension des flux de données adressés à un destinataire situé dans un pays tiers ou à une organisation internationale.* »

81. L'article 83 du RGPD prévoit que chaque autorité de contrôle veille à ce que les amendes administratives imposées soient, dans chaque cas, effectives, proportionnées et dissuasives, avant de préciser les éléments qui doivent être pris en compte pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de cette amende :

*a) la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi ;*

*b) le fait que la violation a été commise délibérément ou par négligence ;*

*c) toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées ;*

*d) le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32 ;*

*e) toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant ;*

*f) le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs ;*

*g) les catégories de données à caractère personnel concernées par la violation ;*

*h) la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation ;*

*i) lorsque des mesures visées à l'article 58, paragraphe 2, ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures ;*

*j) l'application de codes de conduite approuvés en application de l'article 40 ou de mécanismes de certification approuvés en application de l'article 42 ; et*

*k) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation* ».

82. La formation restreinte tient à préciser que les faits pris en compte dans le cadre de la présente décision sont ceux constatés au début de l'enquête. Les éventuelles modifications relatives à l'objet de l'enquête intervenues ultérieurement, même si elles permettent d'établir entièrement ou partiellement la conformité, ne permettent pas d'annuler rétroactivement un manquement constaté.

83. Néanmoins, les démarches effectuées par le contrôlé pour se mettre en conformité avec le RGPD au cours de la procédure d'enquête ou pour remédier aux manquements relevés par le chef d'enquête dans la communication des griefs sont prises en compte par la formation restreinte dans le cadre des éventuelles mesures correctrices et/ou de la fixation du montant d'une éventuelle amende administrative à prononcer.

B. En l'espèce

1. Quant à l'imposition d'une amende administrative

84. Dans son courrier complémentaire à la communication des griefs du 3 août 2020, le chef d'enquête propose à la formation restreinte de prononcer à l'encontre du contrôlé une amende administrative portant sur le montant de 17.700 euros.

85. Afin de décider s'il y a lieu d'imposer une amende administrative et pour décider, le cas échéant, du montant de cette amende, la formation restreinte analyse les critères posés par l'article 83.2 du RGPD :

- Quant à la nature et la gravité de la violation [article 83.2 a) du RGPD], en ce qui concerne les manquements aux articles 37.5, 38.2, 38.3, 38.6, 39.1.a) et 39.1.b) du RGPD, la formation restreinte relève que la nomination d'un DPD par un organisme ne saurait être efficiente et efficace, à savoir faciliter le respect du RGPD par l'organisme, que dans le cas où le DPD dispose des qualités professionnelles suffisantes et des ressources nécessaires pour l'exercice de ses missions, exerce ses fonctions et missions en toute indépendance, n'exerce pas d'autres fonctions qui pourraient entraîner un conflit d'intérêts, exerce de façon effective ses missions, dont la mission d'information et de conseil du responsable du traitement et la mission de contrôle du respect du RGPD.

- Quant au critère de durée [article 83.2.a) du RGPD], la formation restreinte relève :

(1) Qu'un nouveau DPD, disposant d'une expertise suffisante en matière de protection des données, a été engagé et nommé par le contrôlé en date du 13 novembre 2019. Le manquement à l'article 37.5 du RGPD a donc duré dans le temps, entre le 25 mai 2018 et le 13 novembre 2019 ;

(2) Qu'il n'a pas été démontré par le contrôlé que le DPD en fonction au moment de l'ouverture de l'enquête disposait des ressources nécessaires pour l'exercice de ses missions et que d'après le courrier du contrôlé du 19 août 2020, le nouveau DPD « *effectue sa mission* (…) *sur une période de 80 % de son temps. Les 20 % restants consistent à assister la […] dans la gestion contractuelle avec les intervenants externes* ». Le manquement à l'article 38.2 du RGPD a donc duré dans le temps, à partir du 25 mai 2018, étant précisé que la formation restreinte n'a pas pu constater que le manquement a pris fin ;

(3) Qu'il n'a pas été démontré par le contrôlé que le DPD en fonction au moment de l'ouverture de l'enquête pouvait accéder directement au plus haut niveau de la direction dès qu'il l'estimait nécessaire. Ceci n'a pas non plus été démontré en ce qui concerne le nouveau DPD. Le manquement à l'article 38.3 du RGPD a donc duré dans le temps, à partir du 25 mai 2018, étant précisé que la formation restreinte n'a pas pu constater que le manquement a pris fin ;

(4) Que le nouveau DPD, engagé et nommé par le contrôlé en date du 13 novembre 2019, n'exerce aucune autre fonction auprès du contrôlé, si ce n'est, d'après le courrier du contrôlé du 19 août 2020, une fonction de support auprès de […] pour la « *gestion contractuelle des intervenants externes* ». Le manquement à l'article 38.6 du RGPD a donc duré dans le temps, entre le 25 mai 2018 et le 13 novembre 2019 ;

(5) Que dans son courrier du 19 août 2020, le contrôlé indique que le nouveau DPD « *a déjà fait modifier différentes procédures internes afin que la protection des données à caractère personnel soit bien prise en compte au sein de nos diverses activités* » et qu'un « *plan de suivi de nos divers traitements, en fonction de leurs sensibilités, a (…) été mis en place* ». Le manquement à l'article 39.1.b) du RGPD a donc duré dans le temps, à tout le moins entre le 25 mai 2018 et le 19 août 2020 ;

(6) Qu'il n'a pas été démontré par le contrôlé que le DPD en fonction au moment de l'ouverture de l'enquête exerçait ses missions d'information et de conseil à l'égard du responsable de traitement, et que, dans sa prise de position du 14 novembre 2019, la fréquence à laquelle les rapports d'activités établis sont adressés à la Direction […] n'a pas été explicitée par le contrôlé. Le manquement à l'article 39.1.a) du RGPD a donc duré dans le temps, à tout le moins entre le 25 mai 2018 et le 14 novembre 2019.

- Quant au degré de coopération établi avec l'autorité de contrôle [article 83.2 f) du RGPD], la formation restreinte tient compte de l'affirmation du chef d'enquête selon laquelle le contrôlé a fait preuve d'une participation constructive tout au long de l'enquête.

- Quant aux catégories de données à caractère personnel concernées par la violation [article 83.2 g) du RGPD], la formation restreinte tient compte du fait que le contrôlé traite des catégories particulières de données à caractère personnel, en particulier des données concernant la santé.

86. La formation restreinte constate que les autres critères de l'article 83.2 du RGPD ne sont ni pertinents, ni susceptibles d'influer sur sa décision quant à l'imposition d'une amende administrative et son montant.

87. La formation restreinte relève que si plusieurs mesures ont été décidées par le contrôlé afin de remédier en totalité ou en partie à certains manquements, celles-ci n'ont été décidées qu'à la suite du lancement de l'enquête par les agents de la CNPD en date du 17 septembre 2018 (voir aussi le point 82 de la présente décision).

88. Dès lors, la formation restreinte considère que le prononcé d'une amende administrative est justifié au regard des critères posés par l'article 83.2 du RGPD pour manquement aux articles 37.5, 38.2, 38.3, 38.6, 39.1.a) et 39.1.b) du RGPD.

89. S'agissant du montant de l'amende administrative, la formation restreinte rappelle que l'article 83.3 du RGPD prévoit qu'en cas de violations multiples, comme c'est le cas en l'espèce, le montant total de l'amende ne peut excéder le montant fixé pour la violation la plus grave. Dans la mesure où un manquement aux articles 37.5, 38.2, 38.3, 38.6, 39.1.a) et 39.1.b) du RGPD est reproché au contrôlé, le montant maximum de l'amende pouvant être retenu s'élève à 10 millions d'euros ou 2% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

90. Au regard des critères pertinents de l'article 83.2 du RGPD évoqués ci-avant, la formation restreinte considère que le prononcé d'une amende de 10.700 euros apparaît à la fois effectif, proportionné et dissuasif, conformément aux exigences de l'article 83.1 du RGPD.

2. <u>Quant à la prise de mesures correctrices</u>

91. Dans son courrier complémentaire à la communication des griefs du 3 août 2020, le chef d'enquête propose à la formation restreinte de prendre les mesures correctrices suivantes :

> « *a) Ordonner la mise en place de mesures permettant au DPD (ou à une équipe " Data Protection " dédiée) d'acquérir une expertise suffisante et adaptée aux besoins du responsable de traitement en matière de protection des données conformément aux dispositions de l'article 37, paragraphe (5) du RGPD et aux lignes directrices relatives*

*au DPD du groupe de travail " article 29 " sur la protection des données qui précisent que le niveau d'expertise du DPD doit être proportionné à la sensibilité, à la complexité et au volume des données traitées par l'organisme. Bien que plusieurs manières puissent être envisagées pour parvenir à ce résultat, une des possibilités pourrait être de désigner un autre DPD qui dispose de l'expertise suffisante. Plusieurs mesures telles que celles reprises ci-dessous peuvent être envisagées pour parvenir à ce résultat:*

*- fournir un support interne ou externe formel à votre DPD en matière de protection des données et de systèmes d'information ;*

*- inscrire votre DPD à des / poursuivre les formations accélérées/intensives en matière de protection des données et de systèmes d'information ;*

*- désigner un autre DPD qui dispose de l'expertise suffisante.*

*b) Ordonner la mise à disposition de ressources nécessaires au DPD conformément aux exigences de l'article 38 paragraphe 2 du RGPD. Bien que plusieurs manières puissent être envisagées pour parvenir à ce résultat, une des possibilités pourrait être de décharger le DPD de tout ou partie de ses autres missions/fonctions et/ou de lui fournir du support formel, en interne ou en externe, quant à l'exercice de ses missions de DPD.*

*c) Ordonner le déploiement effectif d'un mécanisme garantissant l'autonomie du DPD conformément aux exigences de l'article 38 paragraphe 3 du RGPD. Le DPD doit pouvoir intervenir personnellement au plus haut niveau de la hiérarchie. Bien que plusieurs manières puissent être envisagées pour parvenir à ce résultat, une des possibilités pourrait être de s'assurer que le DPD assiste notamment directement au Comité de Direction et aux diverses réunions de projet.*

*d) Ordonner le déploiement de mesures assurant que les différentes missions et tâches de la personne exerçant la fonction de DPD n'entraînent pas de conflits d'intérêts conformément aux exigences de l'article 38 paragraphe 6 du RGPD. Bien que plusieurs manières puissent être envisagées pour parvenir à ce résultat, une des possibilités seraient l'implication d'une tierce personne, bénéficiant des compétences nécessaires, pour la revue des traitements pour lesquels il existe un conflit d'intérêt, à savoir les traitements IT. Une autre possibilité serait de de désigner un DPD qui n'est pas amené à se prononcer sur des traitements qu'il a lui-même mis en place.*

*e) Ordonner le déploiement de la mission de contrôle, conformément à l'article 39 paragraphe 1 b) du RGPD. Bien que plusieurs manières puissent être envisagées pour parvenir à ce résultat, le DPD devrait documenter ses contrôles sur l'application des règles et procédures internes en matière de protection des données (deuxième ligne de défense). Cette documentation pourrait prendre la forme d'un plan de contrôle.* »

92. Quant aux mesures correctrices proposées par le chef d'enquête et par référence au point 83 de la présente décision, la formation restreinte prend en compte les démarches effectuées par le contrôlé afin de se conformer aux dispositions des articles 37.5, 38.2, 38.3, 38.6 et 39.1.b) du RGPD, notamment les mesures décrites dans son courrier du 19 août 2020. Plus particulièrement, elle prend note des faits suivants :

- En ce qui concerne la violation de l'article 37.5 du RGPD, la formation restreinte constate que le contrôlé a procédé à la désignation d'un nouveau DPD disposant d'une expertise suffisante. La formation restreinte considère dès lors qu'il n'y a pas lieu de prononcer la mesure correctrice proposée par le chef d'enquête et reprise sous a) du point 91 de la présente décision.

- En ce qui concerne la violation de l'article 38.2 du RGPD, le contrôlé indique dans son courrier du 19 août 2020 que le nouveau DPD « *effectue sa mission* (…) *sur une période de 80 % de son temps. Les 20 % restants consistent à assister la […] dans la gestion contractuelle avec les intervenants externes* ». Compte tenu du fait que le contrôlé traite un nombre substantiel de données dont le degré de sensibilité peut être relativement élevé, la formation restreinte considère que le DPD devrait disposer de ressources plus élevées pour l'exercice de ses missions. La formation restreinte considère dès lors qu'il y a lieu de prononcer la mesure correctrice proposée par le chef d'enquête et reprise sous b) du point 91 de la présente décision.

- En ce qui concerne la violation de l'article 38.3, la formation retreinte constate que les éléments communiqués par le contrôlé dans son courrier 19 août 2020 ne suffisent pas à démontrer que le DPD est en mesure d'accéder directement au plus haut niveau de la direction dès qu'il l'estime nécessaire. La formation restreinte considère dès lors qu'il y a lieu de prononcer la mesure correctrice proposée par le chef d'enquête et reprise sous c) du point 91 de la présente décision.

- En ce qui concerne la violation de l'article 38.6, la formation restreinte considère que la désignation d'un nouveau DPD n'exerçant aucune autre fonction auprès du contrôlé, si ce n'est, d'après le courrier du contrôlé du 19 août 2020, une fonction de support auprès de […] pour la « *gestion contractuelle des intervenants externes* », permet d'assurer que le DPD ne sera pas amené à se prononcer sur des traitements dont il aurait contribué à déterminer les finalités et les moyens. La formation restreinte considère dès lors qu'il n'y a pas lieu de prononcer la mesure correctrice proposée par le chef d'enquête et reprise sous d) du point 91 de la présente décision.

- En ce qui concerne la violation de l'article 39.1.b) du RGPD, la formation restreinte prend note du fait que dans son courrier du 19 août 2020, le contrôlé indique que le nouveau DPD « *a déjà fait modifier différentes procédures internes afin que la protection des données à caractère personnel soit bien prise en compte au sein de nos diverses activités* » et qu'un « *plan de suivi de nos divers traitements, en fonction de leurs sensibilités, a* (…) *été mis en place* ». Néanmoins, la formation restreinte ne dispose pas de la documentation permettant de démontrer la mise en œuvre de ces mesures. La formation restreinte considère dès lors qu'il y a lieu de prononcer la mesure correctrice proposée par le chef d'enquête et reprise sous e) du point 91 de la présente décision.

**Compte tenu des développements qui précèdent, la Commission nationale siégeant en formation restreinte et délibérant à l'unanimité des voix décide :**

- de retenir les manquements aux articles 37.5, 38.2, 38.3, 38.6, 39.1.a) et 39.1.b) du RGPD ;

- de prononcer à l'encontre de la « Fondation A » une amende administrative d'un montant de dix mille sept cent euros (10.700 euros) au regard de la violation des articles 37.5, 38.2, 38.3, 38.6, 39.1.a) et 39.1.b) du RGPD ;

- de prononcer à l'encontre de la « Fondation A », une injonction de se mettre en conformité avec l'article 38.2 du RGPD, dans un délai de quatre mois suivant la notification de la décision de la formation restreinte, en particulier :

s'assurer que le DPD dispose des ressources nécessaires pour l'exercice de ses missions ;

- de prononcer à l'encontre de la « Fondation A », une injonction de se mettre en conformité avec l'article 38.3 du RGPD, dans un délai de quatre mois suivant la notification de la décision de la formation restreinte, en particulier :

s'assurer de la mise en place et du maintien d'un mécanisme formel garantissant l'autonomie du DPD ;

- de prononcer à l'encontre de la « Fondation A », une injonction de se mettre en conformité avec l'article 39.1.b) du RGPD, dans un délai de quatre mois suivant la notification de la décision de la formation restreinte, en particulier :

s'assurer du déploiement formel et documenté de la mission de contrôle du DPD.

Ainsi décidé à Belvaux en date du 4 août 2021.

La Commission nationale pour la protection des données siégeant en formation restreinte

| | | |
|---|---|---|
| Tine A. Larsen<br>Présidente | Thierry Lallemang<br>Commissaire | Marc Lemmer<br>Commissaire |

**Indication des voies de recours**

La présente décision administrative peut faire l'objet d'un recours en réformation dans les trois mois qui suivent sa notification. Ce recours est à porter devant le tribunal administratif et doit obligatoirement être introduit par le biais d'un avocat à la Cour d'un des Ordres des avocats.