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

Délibération n° 23FR/2021 du 29 juin 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

[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.

(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 l'Administration A (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. […]

4. Par courrier du 17 septembre 2018, le chef d'enquête a envoyé un questionnaire préliminaire au contrôlé auquel ce dernier a répondu par courriel du 5 octobre 2018. Des visites sur place ont eu lieu les 5 mars et 2 mai 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 ;
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 communiquer les coordonnées du DPD à l'autorité de contrôle[3] ;
- l'obligation d'associer le DPD à toutes les questions relatives à la protection des données à caractère personnel[4] ;
- l'obligation de fournir les ressources nécessaires au DPD[5] ;
- l'obligation de garantir l'autonomie du DPD[6] ;
- la mission d'information et de conseil du DPD[7] ;
- la mission de contrôle du DPD[8].

8. Par courrier du 22 novembre 2019, le contrôlé a adressé au chef d'enquête sa prise de position quant aux manquements énumérés 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 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 six mesures correctrices différentes.

[2] Objectif n°4
[3] Objectif n°3
[4] Objectif n°8
[5] Objectif n°6
[6] Objectif n°7
[7] Objectif n°9
[8] Objectif n°10

10. Par courrier du 14 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 des observations orales sur l'affaire 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[9]. 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* »[10] 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* »[11].

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

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* »[12].

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, le chef d'enquête 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 n'a pas de formation initiale en matière juridique ou protection des données, ni ne justifie d'une pratique en la matière. Le fait que le DPD ait participé à 2 formations spécifiques protection des données en 2017 et ait suivi les ateliers participatifs de l'INAP en 2018, ne suffit pas à établir l'existence d'une expertise adaptée aux besoins du responsable de traitement* ».

18. Dans sa prise de position du 22 novembre 2019, le contrôlé fait valoir la volonté et la capacité du DPD d'apprendre et de se familiariser avec de nouvelles législations, son excellente connaissance du mode de fonctionnement du contrôlé et des procédures, son sens aigu des responsabilités ainsi que sa grande conscience professionnelle. […] Par ailleurs, le contrôlé affirme avoir mis en place une collaboration étroite, bien que non-formalisée, avec le service juridique.

19. La formation restreinte relève d'abord que dans sa prise de position du 22 novembre 2019, le contrôlé ne met pas en cause les constatations faites par le chef d'enquête quant à l'absence de formation initiale en matière juridique ou de protection des données du DPD, et quant à l'absence de pratique du DPD en la matière.

20. La formation restreinte prend note du fait que, d'après le contrôlé, le DPD dispose d'une bonne compréhension du fonctionnement ainsi que des procédures du contrôlé, […] et qu'une collaboration étroite a été mise en place entre le DPD et le service juridique.

[12] WP 243 v.01, version révisée et adoptée le 5 avril 2017, p.14

Néanmoins, la formation restreinte considère que ces éléments ne permettent pas d'établir que le DPD dispose d'une expertise adaptée aux besoins du contrôlé, notamment au vu de la sensibilité, de la complexité et du volume des données traitées par le contrôlé. En effet, Il ressort de la communication des griefs que le contrôlé « *gère environ […] clients […]. L'Administration A emploie par ailleurs environ […] collaborateurs. L'organisme traite donc un nombre substantiel de données dont le degré de sensibilité peut être relativement élevé […].* »

21. La formation restreinte prend par ailleurs note du fait que dans son courrier du 14 août 2020, le contrôlé a indiqué être « *en train de finaliser le recrutement d'un DPO à temps plein et disposant d'un niveau d'expertise adapté à la sensibilité, à la complexité et au volume des données traitées* [par le contrôlé]. » 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.

22. La formation restreinte relève en outre que si elle a pu constater qu'un nouveau DPD a effectivement été désigné par le contrôlé en cours d'enquête, elle ne dispose néanmoins pas de la documentation qui permettrait de vérifier qu'il dispose des 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. <u>Sur le manquement à l'obligation de communiquer les coordonnées du DPD à l'autorité de contrôle</u>

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

24. L'article 37.7 du RGPD prévoit l'obligation pour l'organisme de communiquer les coordonnées du DPD à l'autorité de contrôle. En effet, il résulte de l'article 39.1. e) du RGPD que le DPD fait office de point de contact pour l'autorité de contrôle de sorte qu'il est important que cette dernière dispose des coordonnées du DPD.

25. Les lignes directrices concernant les DPD expliquent à cet égard que cette exigence vise à garantir que « *les autorités de contrôle puissent aisément et directement prendre contact avec le DPD sans devoir s'adresser à un autre service de l'organisme* »[13].

26. Il convient encore de noter que la CNPD a publié sur son site Internet dès le 18 mai 2018 un formulaire permettant aux organismes de lui transmettre les coordonnées de leur DPD.

2. <u>En l'espèce</u>

27. Il résulte du rapport d'audit que, pour que le chef d'enquête considère l'objectif 3 comme rempli par le contrôlé dans le cadre de cette campagne d'audit, le chef d'enquête s'attend à ce que l'organisme ait communiqué au 25 mai 2018 les coordonnées de son DPD à la CNPD.

28. Selon la communication des griefs, page 3, la communication des coordonnées du DPD à la CNPD a été faite le […] octobre 2018 par l'intermédiaire du Commissariat du Gouvernement à la protection des données auprès de l'État, et non pas par le contrôlé lui-même.

29. Dans sa prise de position du 22 novembre 2019, le contrôlé prend acte que la communication des coordonnées du DPD n'a pas été faite selon la procédure prévue et affirme qu'il veillera à l'avenir à ce que tout changement éventuel concernant le DPD soit communiqué directement à la CNPD.

30. La formation restreinte constate que le RGPD est applicable depuis le 25 mai 2018 de sorte que l'obligation de communiquer les coordonnées du DPD à l'autorité de contrôle existe depuis cette date. Ainsi, la communication des coordonnées du DPD à la CNPD en date du […] octobre 2018 était tardive. Par ailleurs, il y a lieu de souligner qu'il appartient à l'organisme ayant désigné le DPD de communiquer lui-même les coordonnées de son DPD à la CNPD, même si l'organisme est, comme en l'espèce, une administration de l'Etat.

31. Au vu de ce qui précède, la formation restreinte conclut que l'article 37.7 du RGPD n'a pas été respecté par le contrôlé.

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

C. Sur le manquement à l'obligation d'associer le DPD à toutes les questions relatives à la protection des données à caractère personnel

1. Sur les principes

32. Selon l'article 38.1 du RGPD, l'organisme doit veiller à ce que le DPD soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

33. Les lignes directrices concernant les DPD précisent qu'*« [i]l est essentiel que le DPD, ou son équipe, soit associé dès le stade le plus précoce possible à toutes les questions relatives à la protection des données. […] L'information et la consultation du DPD dès le début permettront de faciliter le respect du RGPD et d'encourager une approche fondée sur la protection des données dès la conception; il devrait donc s'agir d'une procédure habituelle au sein de la gouvernance de l'organisme. En outre, il importe que le DPD soit considéré comme un interlocuteur au sein de l'organisme et qu'il soit membre des groupes de travail consacrés aux activités de traitement de données au sein de l'organisme*»[14].

34. Les lignes directrices concernant les DPD fournissent des exemples sur la manière d'assurer cette association du DPD, tels que :

- d'inviter le DPD à participer régulièrement aux réunions de l'encadrement supérieur et intermédiaire ;
- de recommander la présence du DPD lorsque des décisions ayant des implications en matière de protection des données sont prises ;
- de prendre toujours dûment en considération l'avis du DPD ;
- de consulter immédiatement le DPD lorsqu'une violation de données ou un autre incident se produit.

35. Selon les lignes directrices concernant les DPD, l'organisme pourrait, le cas échéant, élaborer des lignes directrices ou des programmes en matière de protection des données indiquant les cas dans lesquels le DPD doit être consulté.

[14] WP 243 v.01, version révisée et adoptée le 5 avril 2017, p. 16

2. <u>En l'espèce</u>

36. Il ressort du rapport d'audit que, pour que le chef d'enquête considère l'objectif 8 comme rempli par le contrôlé dans le cadre de cette campagne d'audit, il s'attend à ce que le DPD participe de manière formalisée et sur base d'une fréquence définie au Comité de Direction, aux comités de coordination de projet, aux comités de nouveaux produits, aux comités sécurité ou tout autre comité jugé utile dans le cadre de la protection des données.

37. Selon la communication des griefs, pages 3 et 4, le DPD est informé des nouveaux projets de façon informelle et fait un point informel sur les questions de protection des données avec [la Direction] du contrôlé tous les 15 jours. La communication des griefs indique encore que « *[l]e fait que l'intégration d'un module GDPR dans la méthodologie projet soit en cours ne suffit pas à établir l'existence d'une association organisée du DPD aux questions relatives à la protection des données, ni n'est de nature à établir le positionnement du DPD en tant qu'interlocuteur au sein de l'organisme.* »

38. Dans sa prise de position du 22 novembre 2019, le contrôlé fait valoir qu'il s'agit avant tout d'un manque de formalisation de sa part et que le DPD est associé aux questions relatives à la protection des données personnelles dans la mesure où il est consulté par les chefs de projets et la direction « *dès qu'ils identifient des activités de traitement qui risquent de comporter des données à caractère personnel* ». D'après le contrôlé, le DPD est également invité « *à toutes les réunions dans lesquelles des questions relatives à la protection des données à caractère personnel sont à l'ordre du jour, y compris le comité de direction* ». Par ailleurs, le contrôlé indique que le DPD répond à toute question de la part des collaborateurs du contrôlé à ce sujet.

39. La formation restreinte reconnait que le RGPD ne précise pas quelles sont les mesures qui devraient être prises par le responsable du traitement pour assurer l'association du DPD à toutes les questions relatives à la protection des données. Les lignes directrices concernant les DPD formulent toutefois des recommandations et des bonnes pratiques, afin de guider les responsables du traitement dans la mise en conformité à l'égard de leur gouvernance en fournissant notamment des exemples sur la manière d'assurer cette association.

40. La formation restreinte relève d'ailleurs 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. »

41. Or, la formation restreinte constate qu'il est aussi précisé dans la communication des griefs que le contrôlé « *gère environ […] clients […].* [Le contrôlé] *emploie par ailleurs environ […] collaborateurs. »* Le chef d'enquête en conclut que *« L'organisme traite donc un nombre substantiel de données dont le degré de sensibilité peut être relativement élevé, tels que […].* » La formation restreinte partage cette appréciation. La formation restreinte considère dès lors que la participation formalisée et systématique du DPD aux réunions pertinentes, telle qu'elle est attendue par le chef d'enquête, constitue une mesure proportionnée afin d'assurer l'association du DPD à toutes les questions relatives à la protection des données des personnelles.

42. La formation restreinte prend note du fait que dans sa prise de position du 22 novembre 2019, le contrôlé indique qu'il a été décidé « *de formaliser davantage la participation* [du] *DPD aux activités.* [Le DPD] *est ainsi désormais d'office membre du comité de pilotage de tous les projets* [du contrôlé] *(projets déjà en cours et nouveaux projets)* » et prend aussi note du fait que dans son courrier du 14 août 2020, le contrôlé précise en outre qu'en cas d'absence du DPD dans une réunion *« le compte rendu lui est envoyé et le cas échéant une entrevue entre le chef de projet et le DPO est organisée.* » Si ces mesures devraient faciliter l'association du DPD à toutes les questions relatives à la protection des données, il convient néanmoins de constater que celles-ci ont été décidées 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 responsable de traitement n'a pas été en mesure de démontrer que le DPD était associé de manière approprié, à toutes les questions relatives à la protection des données personnelles.

43. La formation restreinte constate en outre qu'elle ne dispose pas de la documentation qui permettrait de démontrer que les mesures décrites par le contrôlé auraient été mises en œuvre.

44. Au vu de ce qui précède, la formation restreinte conclut que l'article 38.1 du RGPD n'a pas été respecté.

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

1. Sur les principes

45. 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.* »

46. Il résulte des lignes directrices concernant les DPD que les aspects suivants doivent notamment être pris en considération[15] :

- « *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* ».

47. 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 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.* »

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

2. <u>En l'espèce</u>

48. 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, le chef d'enquête 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.

49. Selon la communication des griefs, page 4, *« [i]l ressort de l'enquête que le DPD est affecté à 25% (environ 10h par semaine). Le DPD exerce seul ses missions. Le fait que le DPD bénéficie du support informel du service juridique et du service informatique et le fait qu'un prestataire externe soit intervenu à raison de 60 jours homme sur une période de 12 mois (soit environ 5 jours par mois), ne sauraient suffire à fournir un temps suffisant pour que le DPD accomplisse ses missions.* » La communication des griefs indique ensuite que « *le responsable de traitement n'a pas été en mesure de démontrer l'accomplissement des missions de contrôle ou d'information et de conseil du DPD (voir développement au point 3). Cette constatation est de nature à mettre en évidence une inadéquation entre les ressources et moyens mis à disposition du DPD et les besoins du responsable de traitement.* »

50. Dans sa prise de position du 22 novembre 2019, le contrôlé prend acte du constat fait par le chef d'enquête selon lequel le DPD ne dispose pas des ressources nécessaires pour accomplir ses missions. Le contrôlé soutient toutefois que « *même si elle est informelle, la collaboration avec le Service juridique est réelle et permet à notre DPD de bénéficier de ressources supplémentaires ».* D'après le contrôlé, ces ressources sont estimées à environ 5 heures par semaine.

51. La formation restreinte constate qu'il ressort du dossier d'enquête que le DPD était également chef du service […] et consacrait environ 10 heures par semaine à ses tâches de DPD. Même en prenant en considération le support fourni par le service juridique et le service informatique ainsi que l'intervention temporaire d'un prestataire externe, la formation restreinte considère que le DPD ne disposait pas du temps suffisant pour accomplir ses tâches, ceci notamment au regard de la sensibilité, de la complexité et du volume des données traitées par le contrôlé.

52. Dans son courrier du 14 août 2020, le contrôlé indique qu'un DPD à temps plein est en cours de recrutement, qu'il « *disposera du support en interne (du service juridique, du service*

informatique et de la DPO actuelle) » et qu'une enveloppe budgétaire est envisagée pour un support externe.

53. 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 en particulier que le DPD exerce ses fonctions à temps plein.

54. 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.

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

1. Sur les principes

55. 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.

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

57. Selon les lignes directrices concernant les DPD[16], 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 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*

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

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>

58. 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, le chef d'enquête s'attend à ce que le DPD soit « *rattaché au plus haut niveau de la direction afin de garantir au maximum son autonomie* ».

59. Selon la communication des griefs, p. 4, « *[i]l ressort de l'enquête que le DPD était initialement rattaché au directeur adjoint, rattachement qui n'était pas formalisé. Par ailleurs, l'Administration A n'a pas été en mesure de démontrer l'existence d'un rapport direct au niveau le plus élevé de la direction. Il n'existe notamment pas d'outil, tel qu'un rapport d'activité, qui aurait pu permettre au DPD d'adresser des conseils formels au responsable de traitement. En cours d'enquête, l'Administration a présenté aux agents de la CNPD un organigramme montrant le rattachement du DPD directement à [la Direction]. Cette modification permet, certes de documenter la volonté de l'organisme de se conformer, mais cette modification ne suffit pas à elle seule à lever le manquement, toutefois constaté au début de l'enquête. En effet, le responsable de traitement n'a pas été en mesure de démontrer que le DPD pouvait agir sans recevoir d'instruction en ce qui concerne l'exercice de ses missions.* »

60. Dans sa prise de position du 22 novembre 2019, le contrôlé fait valoir que le DPD est désormais formellement rattachée directement à la [Direction] du contrôlé dans l'organigramme et affirme notamment que le DPD « *ne reçoit pas d'instructions en ce qui concerne l'exercice de ses missions visées à l'article 39, et elle obtient le soutien du responsable du traitement afin de pouvoir les exercer en autonomie* ».

61. Quant à la possibilité pour le DPD d'adresser des conseils formels qui contribuerait à démontrer, selon les termes du chef d'enquête, *« l'existence d'un rapport direct au niveau le plus élevé de la direction »*, la formation restreinte constate qu'il ressort du dossier d'enquête que le DPD participe à des réunions informelles avec la direction[17] et que le DPD fait un point informel sur les questions de protection des données avec la [Direction] tous les 15 jours[18].

[17] Compte-rendu de visite du 5 mars 2019, point 8
[18] Communication des griefs, p. 3

La formation restreinte relève que, compte tenu du caractère informel de ces contacts du DPD avec la direction, ces éléments ne tendent pas à démontrer l'existence d'un rapport direct au niveau le plus élevé de la direction.

62. Par ailleurs, pour ce qui est du rattachement hiérarchique, 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 40 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.* »

63. Or, tel que cela est mentionné au point 41 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 […]* ». La formation restreinte considère dès lors que, en l'absence d'autres mesures qui permettraient de démontrer que le DPD est en mesure de contourner les niveaux hiérarchiques intermédiaires 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 que le rattachement du DPD au plus haut niveau de la direction n'a été décidé par le contrôlé qu'après le début de l'enquête.

64. Au vu de ce qui précède, la formation restreinte se rallie 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 pouvait agir sans recevoir d'instruction en ce qui concerne l'exercice de ses missions.

65. 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.

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

1. Sur les principes

66. 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

67. 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* ».

68. Sur ces deux points, selon la communication des griefs, page 5, « *[i]l ressort de l'enquête qu'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. Par ailleurs, le personnel de l'Administration A reçoit des séances de sensibilisation relatives à la sécurité informatique, mais pas de sensibilisation sur la protection des données en général. Le responsable de traitement n'a pas été en mesure de démontrer que le DPD exerce ses missions d'information et de conseil, tant à l'égard du responsable de traitement lui-même qu'à l'égard des employés qui effectuent les opérations de traitement.* »

69. Dans sa prise de position du 22 novembre 2019, le contrôlé fait valoir que le DPD a conseillé la direction de l'organisme sur les obligations lui incombant en matière de protection des données, « *même si ces conseils n'étaient pas formellement documentés* ». Le contrôlé indique encore qu' « *[u]n projet de mise en conformité avec le RGPD a été lancé en 2017 et différentes étapes ont été listées sur un graphique qui servait de base à la DPD et à la Direction pour définir les priorités. La progression du projet n'a par contre effectivement pas fait l'objet d'une documentation.* » […] Enfin, le contrôlé soutient que le DPD a conseillé ses agents pour toute question relative à la protection des données, « *même si des formations spécifiques sur ce sujet n'ont pas encore eu lieu* » et indique que « [l]*es chefs de service et les collaborateurs*

ont été encouragés à contacter individuellement le DPD pour toute information et tout conseil au sujet de la protection des données. »

70. 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*.[19] »

71. En ce qui concerne la mission d'information et de conseil à l'égard du responsable du traitement, il ressort du dossier d'enquête que le DPD a été impliqué dans l'établissement du registre des activités de traitement[20], qu'il participe à des réunions informelles avec la direction[21], que l'accès à la direction est aisé pour le DPD[22] et que le DPD fait un point informel sur les questions de protection des données avec la [Direction] tous les 15 jours[23].

72. Néanmoins, la formation restreinte rappelle qu'elle a déjà constaté au point 40 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 41 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 […]* ». La formation restreinte

[19] WP 243 v.01, version révisée et adoptée le 5 avril 2017, p. 22
[20] Compte-rendu de visite du 5 mars 2019, p. 2
[21] Compte-rendu de visite du 5 mars 2019, point 8
[22] Compte-rendu de visite du 5 mars 2019, point 8
[23] Communication des griefs, p. 3

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

74. La formation restreinte prend note du fait que le contrôlé a indiqué dans son courrier du 14 août 2020 qu'il a été décidé de mettre en place un reporting formel des activités du DPD (sur une base trimestrielle susceptible d'être revue et adaptée en cas de besoin). La formation restreinte, qui ne dispose pas de la documentation qui permettrait de démontrer la mise en œuvre de cette mesure, constate que celle-ci a été décidée en cours d'enquête et 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.

75. Quant à la mission d'information et de conseil à l'égard des employés, la formation restreinte constate qu'il ressort du dossier d'enquête[24] que :

- environ […] agents du contrôlé ont été formés à la sécurité informatique ;
- le code de conduite et la formation relative à […] contiennent des éléments relatifs à la protection des données personnelles ;
- le personnel affecté […] du contrôlé a été formé pour prévenir la divulgation non autorisée d'information ; et
- un plan de formation intégrant des aspects relatifs à la protection des données et à destination de tous les agents du contrôlé est prévu pour fin 2019/début 2020.

76. Dans sa prise de position du 22 novembre 2019, le contrôlé indique que « *Des formations spécifiques portant sur la protection des données personnelles sont en train d'être organisées et auront lieu en 2020.* »

77. La formation restreinte constate aussi que le contrôlé a indiqué dans son courrier du 14 août 2020 que « [l]*es formations internes des collaborateurs au sujet du RGPD et de la protection des données* (…) *ont débuté au cours du premier trimestre de l'année 2020* » et que ces formations « *sont obligatoires pour tous les collaborateurs et seront organisées de manière régulière* ». La formation restreinte relève néanmoins qu'elle ne dispose pas de la documentation qui permettrait de démontrer la mise en œuvre de cette mesure.

[24] Compte-rendu de visite du 5 mars 2019, point 9

78. Compte tenu des éléments susmentionnés au point 75 de la présente décision qui ressortent du dossier d'enquête ainsi que des indications fournies par le contrôlé dans sa prise de position du 22 novembre 2019 et dans son courrier du 14 août 2020, la formation restreinte constate que, au moment de l'ouverture de l'enquête, le personnel du contrôlé n'était pas spécifiquement sensibilisé à la protection des données.

79. 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 exerce ses missions d'information et de conseil à l'égard des employés qui effectuent les opérations de traitement.

80. La formation restreinte rappelle en outre qu'elle ne dispose pas de la documentation qui permettrait de démontrer que les mesures décidées par le contrôlé, mentionnées aux points 74 et 77 de la présente décision, aient été mises en œuvre.

81. 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.

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

1. Sur les principes

82. 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.

83. Il résulte des lignes directrices concernant les DPD[25] 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;

[25] 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>

84. 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)* ».

85. Selon la communication des griefs, p. 5, *« [i]l ressort de l'enquête que l'organisme ne surveille pas le respect des règles du GDPR et ne dispose pas de plan de contrôle.* » Le chef d'enquête renvoie en particulier à la réponse fournie par le contrôlé à la question 5 c) du questionnaire préliminaire[26]. Le contrôlé y indique qu' *« [a]ctuellement la surveillance du respect des règles ne s'applique pas, un plan d'audit sera établi en 2019.* »

86. Dans sa prise de position du 22 novembre 2019, le contrôlé fait valoir que le DPD était au moment de l'enquête en train d'écrire […] un [document] […] qui « *correspond à un plan de contrôle, puisqu'il analyse les obligations que le RGPD impose au responsable du traitement et explique les démarches entreprises pour se conformer et des actions qui restent à être mises en place* ». Le contrôlé indique que « *ces actions n'ont pas été formellement adressées au responsable du traitement, p.ex. au moyen d'un plan d'action, mais les points les plus urgents ont été soulevés lors des échanges entre la [Direction] et le DPD* ». Le contrôlé indique aussi que « [l]*e DPD s'assure en fin d'année si les actions de conformité signalées aux différents services ont été mis en place* » et que « *les résultats de ces vérifications seront documentés dans un rapport d'audit.* »

87. 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*

[26] Comment le DPD assure-t-il la surveillance du respect des règles ? Veuillez décrire, svp

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.[27] »

88. La formation restreinte a déjà relevé au point 71 de la présent décision qu'il ressort du dossier d'enquête que le DPD était impliqué dans l'établissement du registre des activités de traitement[28]. La formation restreinte relève néanmoins que cet élément pris isolément ne suffit pas à démontrer que le DPD effectue sa mission de contrôle du respect du RGPD de manière adéquate.

89. La formation restreinte rappelle qu'elle a relevé au point 40 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.* »

90. Or, tel que cela est mentionné au point 41 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 […]* ».

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

92. Or, il ressort du dossier d'enquête et des éléments communiqués par le contrôlé dans sa prise de position du 22 novembre 2019 que la mission de contrôlé effectuée par le DPD n'était pas formalisée au moment de l'ouverture de l'enquête.

93. La formation restreinte prend note du fait que dans son courrier du 14 août 2020, le contrôlé indique que « [l]*a mesure d'ordonner le déploiement de la mission de contrôle du DPD par le biais d'un plan de contrôle et des rapports de contrôle est retenue. Un plan de contrôle annuel devra être fourni par le* [DPD] *à la fin de chaque année pour l'année suivante, ensemble avec les rapports de contrôle de l'année écoulée.* » Néanmoins, cette décision étant intervenue

[27] WP 243 v.01, version révisée et adoptée le 5 avril 2017, p. 22
[28] Compte-rendu de visite du 5 mars 2019, p. 2

en cours d'enquête, la formation restreinte se rallie au constat du chef d'enquête selon lequel le contrôlé n'a pas été en mesure de démontrer que le DPD exerce ses missions de contrôle du respect du RGPD.

94. La formation restreinte constate en outre qu'elle ne dispose pas de la documentation qui permettrait de démontrer que cette mesure ait été mise en place par le contrôlé.

95. 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

A. Les principes

96. 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.* »

97. Parmi ces mesures figure aussi le pouvoir d'« *imposer une amende administrative en application de l'article 83 (…)* ». Or, l'article 48, paragraphe 1, 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 précise que *« [l]a CNPD peut imposer les amendes administratives telles que prévues à l'article 83 du [RGPD], sauf à l'encontre de l'État ou des communes* » (soulignement ajouté).

98. 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. 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 à prononcer.

B. En l'espèce

1. Quant à la prise de mesures correctrices

99. 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 l'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 consisterait à fournir un support interne ou externe formel au DPD en matière juridique et en sécurité des système d'information.*

b) Ordonner la mise en place de mesures assurant que pour toute modification ultérieure du DPD, la déclaration auprès de l'autorité de protection des données soit faite dans les temps par le responsable de traitement lui-même, conformément à l'article 37 paragraphe (7) du RGPD.

c) Ordonner la mise en place de mesures assurant une association formelle et effective du DPD à toutes les questions relatives à la protection des données, conformément aux exigences de l'article 38 paragraphe 1 du RGPD. Bien que plusieurs manières puissent être envisagées pour parvenir à ce résultat, une des possibilités consisterait à analyser, avec le DPD, tous les comités/groupes de travail pertinents au regard de la protection des données et de formaliser les modalités de son intervention (information antérieure de l'agenda des réunions, invitation, fréquence, statut de membre permanent, etc...).

d) Ordonner la mise à disposition des 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 consisterait à décharger le DPD de tout ou partie de ses autres missions/fonctions ou de lui fournir un support formel, en interne ou en externe, quant à l'exercice de ses missions de DPD.

e) Ordonner le déploiement de la mission de contrôle du DPD, 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 suid de rapports de contrôle ou d'audit.

f) Ordonner la mise en place de mesures permettant au DPD d'informer et de conseiller formellement le responsable de traitement et les employés (qui procèdent aux traitements) sur leurs obligations en matière de protection des données, conformément à l'article 39 paragraphe 1 a) du RGPD. Bien que plusieurs manières puissent être envisagées pour parvenir à ce résultat, une des possibilités serait de mettre en place un reporting formel des activités du DPD vers la Direction sur base d'une fréquence définie. D'autre part, concernant l'information aux employés, une possibilité serait de mettre en place un dispositif de formation adéquat du personnel en matière de protection des données. »

100. Quant aux mesures correctrices proposées par le chef d'enquête et par référence au point 98 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, 37.7, 38.1, 38.2, 39.1.a et 39.1.b du RGPD, notamment les mesures décrites dans son courrier du 14 août 2020. Plus particulièrement, elle prend note des faits suivants :

- En ce qui concerne la violation de l'article 37.5 du RGPD, le contrôlé a indiqué être « *en train de finaliser le recrutement d'un DPO à temps plein et disposant d'un niveau d'expertise adapté à la sensibilité, à la complexité et au volume des données traitées* [par le contrôlé]. » Si la formation restreinte a pu vérifier qu'un nouveau DPD a été désigné par le contrôlé, elle ne dispose néanmoins pas de la documentation qui permettrait de vérifier qu'il dispose des qualités professionnelles suffisantes. La formation restreinte considère dès lors qu'il y a lieu de prononcer la mesure correctrice proposée par le chef d'enquête sous a).

- En ce qui concerne la violation de l'article 37.7 du RGPD, la formation restreinte a pu vérifier que les coordonnées du nouveau DPD désigné par la contrôlé ont été communiquées conformément à l'article 37.7 du RGPD. La formation restreinte considère dès lors qu'il n'y a pas lieu de prononcer la mesure correctrice proposée par le chef d'enquête sous b).

- En ce qui concerne la violation de l'article 38.1, des mesures ont été décidées par le contrôlé afin d'assurer l'association du DPD à toutes les questions relatives à la protection des données. En effet, le contrôlé a décidé de « *de formaliser davantage la participation* [du] *DPD aux activités.* [Le DPD] *est ainsi désormais d'office membre du comité de pilotage de tous les projets* [du contrôlé*] (projets déjà en cours et nouveaux projets)* » et a précisé qu'en cas d'absence du DPD dans une réunion « *le compte rendu lui est envoyé et le cas échéant une entrevue entre le chef de projet et le DPO est organisée.* » Néanmoins, la formation restreinte ne dispose pas de la documentation permettant de démontrer la prise de telles mesures de mise en conformité par le contrôlé. La formation restreinte considère dès lors qu'il y a lieu de prononcer la mesure correctrice proposée par le chef d'enquête sous c).

- En ce qui concerne la violation de l'article 38.2, le contrôlé a indiqué qu'un DPD « *à temps plein est en train d'être recruté* », qu'il « *disposera du support en interne (du service juridique, du service informatique et de la DPO actuelle*) » et qu'une enveloppe budgétaire était envisagée pour un support externe. Si la formation restreinte a pu vérifier qu'un nouveau DPD a été désigné par le contrôlé en cours d'enquête, elle ne dispose néanmoins pas de la documentation qui permettrait de vérifier qu'il dispose de ressources suffisantes, et en particulier que le DPD exerce ses fonctions à temps plein. La formation restreinte considère dès lors qu'il y a lieu de prononcer la mesure correctrice proposée par le chef d'enquête sous d).

- En ce qui concerne la violation de l'article 39.1.a du RGPD, pour ce qui est de la mission d'information et de conseil à l'égard du responsable du traitement, le contrôlé a indiqué qu'il a été décidé de mettre en place un reporting formel des activités du DPD (sur une base trimestrielle susceptible d'être revue et adaptée en cas de besoin). Pour ce qui est de la mission d'information et de conseil à l'égard des employés, le contrôlé a indiqué que « [l]*es formations internes des collaborateurs au sujet du RGPD et de la protection des données* (…) *ont débuté au cours du premier trimestre de l'année 2020* » et que ces formations « *sont obligatoires pour tous les collaborateurs et seront organisées de manière*

régulière ». Néanmoins, la formation restreinte ne dispose pas de la documentation permettant de démontrer la mise en œuvre de ces mesures de mise en conformité par le contrôlé. La formation restreinte considère dès lors qu'il y a lieu de prononcer la mesure correctrice proposée par le chef d'enquête sous f).

- En ce qui concerne la violation de l'article 39.1.b du RGPD, le contrôlé a indiqué que « [l]*a mesure d'ordonner le déploiement de la mission de contrôle du DPD par le biais d'un plan de contrôle et des rapports de contrôle est retenue. Un plan de contrôle annuel devra être fourni par le* [DPD] *à la fin de chaque année pour l'année suivante, ensemble avec les rapports de contrôle de l'année écoulée.* ». Néanmoins, la formation restreinte ne dispose pas de la documentation permettant de démontrer la mise en œuvre de cette mesure de mise en conformité par le contrôlé. La formation restreinte considère dès lors qu'il y a lieu de prononcer la mesure correctrice proposée par le chef d'enquête sous e).

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, 37.7, 38.1, 38.2, 38.3, 39.1 a) et 39.1 b) du RGPD ;

- de prononcer à l'encontre de l'Administration A, une injonction de se mettre en conformité avec l'article 37.5 du RGPD, dans un délai de quatre mois suivant la notification de la décision de la formation restreinte, les justificatifs de la mise en conformité devant être adressés à la formation restreinte au plus tard dans ce délai, en particulier :

s'assurer que le DPD dispose des qualités professionnelles suffisantes pour exercer ses missions ;

- de prononcer à l'encontre de l'Administration A, une injonction de se mettre en conformité avec l'article 38.1 du RGPD, dans un délai de quatre mois suivant la notification de la décision de la formation restreinte, les justificatifs de la mise en conformité devant être adressés à la formation restreinte au plus tard dans ce délai, en particulier :

s'assurer de l'association formalisée et documentée du DPD à toutes les questions relatives à la protection des données ;

- de prononcer à l'encontre de l'Administration 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, les justificatifs de la mise en conformité devant être adressés à la formation restreinte au plus tard dans ce délai, en particulier :

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

- de prononcer à l'encontre de l'Administration A, une injonction de se mettre en conformité avec l'article 39.1.a du RGPD, dans un délai de quatre mois suivant la notification de la décision de la formation restreinte, les justificatifs de la mise en conformité devant être adressés à la formation restreinte au plus tard dans ce délai, en particulier :

s'assurer que le DPD exerce, de façon formelle et documentée, sa mission d'information et de conseil à l'égard du responsable du traitement ainsi qu'à l'égard des employés ;

- de prononcer à l'encontre de l'Administration 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, les justificatifs de la mise en conformité devant être adressés à la formation restreinte au plus tard dans ce délai, en particulier :

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

Ainsi décidé à Belvaux en date du 29 juin 2021.

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

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Marc Lemmer 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.