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

Délibération n° 36FR/2021 du 13 octobre 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 la Société A située au […], L-[…] et enregistrée au registre du commerce et des sociétés luxembourgeois sous le n°B[…] (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 3 de ses statuts, le contrôlé [a pour objet de faire, pour elle ou pour compte de tiers, toutes opérations d'assurance et de coassurance dans toutes les branches d'assurance autres que la branche vie] […].

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. Des visites sur place ont eu lieu le 21 janvier et le 23 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 11 novembre 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 d'associer le DPD à toutes les questions relatives à la protection des données[3] ;
- l'obligation de fournir les ressources nécessaires au DPD[4] ;
- la mission de contrôle du DPD[5].

8. Le 10 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 4 mesures correctrices différentes ainsi que d'infliger au contrôlé une amende administrative d'un montant de 23.400 euros.

9. Par courrier du 16 septembre 2020, le contrôlé a fait parvenir au chef d'enquête ses observations quant au courrier complémentaire à la communication des griefs.

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

10. L'affaire a été à l'ordre du jour de la séance de la formation restreinte du 26 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

11. 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 […]* ».

12. 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* ».

13. 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[6]. 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* »[7] 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* »[8].

14. 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*

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

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 »[9].

2. <u>En l'espèce</u>

15. Il ressort 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.

16. D'après la communication des griefs, page 3, le DPD du contrôlé, juriste de formation, était absent pour une durée prolongée au moment de l'audit, son retour ayant été prévu pour le début de l'année 2020. Il est précisé que sur base de l'analyse de son CV, « *les agents de la CNPD n'ont pas pu identifier d'expérience particulière en matière de protection des données* ». La communication des griefs indique en outre que « [s]*ur base des échanges avec l'organisme, le DPD n'avait pas d'expertise particulière dans le domaine de la protection des données au moment de sa nomination. Le principal critère pour sa nomination au poste de DPD a été sa fonction de Chief Compliance & Legal Officer* ».

17. Le chef d'enquête précise ensuite qu'en l'absence du DPD, un vice-DPD assure les fonctions de DPD par intérim, que ce dernier dispose de « *nombreuses années d'expérience dans le domaine de la protection des données et en matière juridique, ainsi qu'une longue expérience du secteur d'activité* » et qu'il « *peut bénéficier sur demande de l'aide d'une personne de l'équipe […] IT […]* ».

18. Dans son courrier du 16 septembre 2020, le contrôlé apporte des précisions quant à l'expérience professionnelle du DPD et soutient que le DPD disposait de quatre ans d'expérience en matière de protection des données au moment de l'ouverture de l'enquête. Le contrôlé précise que l'expérience professionnelle du DPD n'avait pas pu être explicitée lors de précédents échanges en raison de l'absence prolongée du DPD ; il n'aurait donc pu fournir, en 2019, que « *son CV non détaillé et très succinct* ».

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

19. Faisant suite à la séance de la formation restreinte du 26 janvier 2021, le contrôlé a fait parvenir à la formation restreinte, en date du 5 février 2021, des pièces complémentaires concernant notamment l'expérience professionnelle du DPD. Il en ressort que le DPD disposait de plus de trois ans d'expérience en matière de protection des données au moment de l'ouverture de l'enquête.

20. La formation restreinte relève 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 « *compte environ […] employés et […] clients* ». Le chef d'enquête en conclut que le contrôlé traite un nombre significatif de données personnelles. La formation restreinte partage cette appréciation et considère que l'attente du chef d'enquête relative au niveau d'expertise du DPD est proportionnée au volume des données traitées.

22. La formation restreinte constate que les précisions relatives à l'expérience professionnelle du DPD n'ont été apportées par le contrôlé seulement qu'après que lui ait été adressé le courrier complémentaire à la communication des griefs ; lors de son enquête, le chef d'enquête a donc pu conclure que, sur base des éléments dont il disposait, l'existence d'une expertise suffisante et adaptée aux besoins du responsable du traitement en matière de protection des données ne pouvait pas être établie. Ceci étant dit, il convient de constater que les précisions apportées par le contrôlé dans son courrier du 16 septembre 2020 ainsi que les pièces complémentaires transmises à la formation restreinte en date du 5 février 2021 permettent de considérer que, au moment de l'ouverture de l'enquête, le DPD disposait d'une expérience suffisante en matière de protection des données.

23. Au vu de ce qui précède, la formation restreinte conclut que le manquement à l'article 37.5 du RGPD n'est pas constitué.

B. 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

24. 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.

25. 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* »[10].

26. 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.

27. 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.

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

2. <u>En l'espèce</u>

28. 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.

29. Selon la communication des griefs, page 4, « [i]*l ressort de l'enquête qu'aucune règle ou fréquence n'a été définie quant à la participation du DPD ou du vice-DPD au Comité de Direction.* » Le chef d'enquête relève en outre que la présence du DPD ou du vice-DPD n'est pas prévue dans le comité « […] » qui se réunit avant chaque lancement d'un nouveau produit. Le chef d'enquête relève enfin que si des mesures visant à mieux associer le DPD ont été proposées par le vice-DPD au Comité de direction, la CNPD n'a pas reçu confirmation que le DPD (ou le vice-DPD) participe de manière formalisée et sur base d'une fréquence définie au Comité de Direction.

30. Dans son courrier du 16 septembre 2020, le contrôlé indique qu'après la fin du projet d'implémentation interne du RGPD (fin janvier 2019), « *il a été convenu avec le* [Comité de direction] *qu'il y aurait des passages ou des communications au [Comité de direction] lorsque nécessaire* » et précise qu'« [i]*l n'a effectivement pas été fixé une régularité automatique* » en ajoutant que « *nous n'avons toutefois pas trouvé un texte légale imposant explicitement un régularité spécifique* ». Le contrôlé a en outre communiqué un inventaire des contacts entre le DPD et le [Comité de direction] pour la période du 1er février 2019 au 31 août 2020. Le contrôlé précise par ailleurs que le « *Risk management »* passe devant le [Comité de direction] plusieurs fois par an dans le cadre de réunions « *[…]* » et consulte le DPD pour préparer ces réunions ; il s'agirait d'une voie supplémentaire de communication du DPD vers le [Comité de direction]. En ce qui concerne le Comité […], le contrôlé indique que sa procédure (dont la dernière version, communiquée à la CNPD, est datée du 11 décembre 2019) prévoit que le DPD « *doit intervenir dans la documentation du dossier produit qui sera soumis lors d'une réunion […] et donner un avis GDPR* ». Le contrôlé précise ensuite que le DPD est « *systématiquement impliqué préalablement à tout lancement de nouveau produit ou de produit existant modifié* ».

31. Il convient de rappeler qu'il a déjà été 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.* »

32. Or, tel que cela est mentionné au point 21 de la présente décision, la formation restreinte partage l'appréciation du chef d'enquête selon laquelle le contrôlé traite un nombre significatif de données personnelles. 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.

33. La formation restreinte prend note du fait que dans son courrier du 16 septembre 2020, le contrôlé indique que « [l]*a fixation d'une régularité constituant une meilleure garantie de collaboration, le [Comité de direction] a validé en date du 16 septembre 2020 la proposition du DPO de prévoir au minimum 4 passages par an au [Comité de direction]* (…) ». Elle prend également note du fait que la procédure du comité […] prévoit, à tout le moins depuis le 11 décembre 2019, une étape de vérification par le DPD pour le lancement de tout nouveau produit ou pour la modification d'un produit existant. Le contrôlé précise toutefois que le « *DPO n'était pas membre permanent [du Comité] […]et n'était pas invité aux réunions […]* » et indique que « *le [Comité de direction] a* (…) *décidé* [le] *16 septembre* [2020] *que le DPO serait désormais membre [du Comité] […]et serait systématiquement invité aux réunions […].* »

34. 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 considère dès lors que, au début de l'enquête, le responsable de traitement n'a pas été en mesure de démontrer que le DPD était associé de manière appropriée à toutes les questions relatives à la protection des données personnelles.

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

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

1. Sur les principes

36. 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.* »

37. Il résulte des lignes directrices concernant les DPD que les aspects suivants doivent notamment être pris en considération[11] :

- « *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* ».

38. 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.* »

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

2. <u>En l'espèce</u>

39. 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.

40. Dans la communication des griefs, page 4, le chef d'enquête indique qu' « *au moment de l'audit, les ressources dédiées à l'équipe en charge de la protection des données étaient d'environ 0.7 ETP, (0.3 pour le vice-DPD et 0.2 pour chacune des deux juristes en charge des demandes des personnes concernées). Le vice-DPD consacre environ deux tiers de son temps à ses fonctions de Tax & Legal Expert et ne peut pas réduire ce temps au profit de la protection des données.* »

41. Le chef d'enquête indique aussi « *qu'il est prévu que le DPD reprenne ses fonctions début 2020* » en relevant que « *le temps qu'il lui sera alloué en matière de protection des données n'est pas encore défini* ». Quant au « vice-DPD », le chef d'enquête prend note du fait qu'il « *peut bénéficier, sur demande, de l'aide d'une personne de l'équipe […] IT […].* »

42. Dans son courrier du 16 septembre 2020, le contrôlé confirme d'abord les constatations faites par le chef d'enquête : « *Il est exact qu'au moment précis du 2ème jour d'audit, le 23 mai 2019, en raison de circonstances exceptionnelles, les ressources étaient temporairement limitées pour le département legal/compliance et DP et que la ressource utilisable globale en DP legal était de 0,7* [ETP]. » Le contrôlé détaille ensuite les circonstances particulières qui ont mené à une limitation des ressources dédiées au DPD ainsi que les mesures qui ont été décidées afin de renforcer ces ressources.

43. Enfin, par courriel du 12 mars 2021, la formation restreinte a été informée que le Comité de direction du contrôlé a décidé, en date du 3 mars 2021, que le DPD exercera ses missions à temps plein (un ETP) au plus tard à compter du début du mois de mai 2021.

44. La formation restreinte prend note des mesures qui ont été décidées par le contrôlé en cours d'enquête afin de renforcer les ressources dédiées au DPD et tient compte du fait que les circonstances particulières qui ont mené à une limitation des ressources dédiées au DPD au début de l'enquête n'étaient pas prévisibles.

45. Au vu de ce qui précède, la formation restreinte conclut que le manquement à l'article 38.2 du RGPD n'est pas constitué.

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

1. Sur les principes

46. 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.

47. Il résulte des lignes directrices concernant les DPD[12] 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;
- informer et conseiller le responsable du traitement ou le sous-traitant et formuler des recommandations à son intention.

2. En l'espèce

48. 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)* ».

49. Selon la communication des griefs, p. 5, *«* [i]*l ressort de l'enquête que l'organisme ne dispose pas de plan de contrôle.*» Le chef d'enquête précise que le vice-DPD a indiqué « *que le suivi des demandes des personnes concernées est déjà opérationnel, via notamment un contrôle régulier des délais des demandes d'accès* ». Le chef d'enquête relève en outre « *que le vice-DPD émet des avis et recommandations »* et que *« le Group Data Protection a réalisé*

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

deux audits au sein de […] la Société A en janvier et en octobre 2018. » Le chef d'enquête constate néanmoins que « *le plan de monitoring relatif à la protection des données était en cours de construction au moment de l'audit*. »

50. Dans son courrier du 16 septembre 2020, le contrôlé indique que l'audit évoqué par la CNPD « *portait sur l'appréciation du projet d'implémentation du RGPD et visait à garantir que* [le contrôlé] *remplisse correctement et pleinement ses obligations* [relatives à la protection des données] ». Il précise qu'« [i]*l y a eu un suivi régulier du Group Audit des points encore ouverts ou à améliorer et donc des échanges entre le DPO et le groupe* ». Le contrôlé indique encore qu'un « *Comité de DPO a été créé au sein du Groupe* » constitué « *du DPO groupe et des DPO des différents business au sein de l'UE, dont le Luxembourg* ». D'après le contrôlé, il s'agit d'un « *outil de contrôle et d'échange d'informations* ». Il relève enfin que « *nous comprenons également qu'il est important, en dehors du suivi de l'audit groupe, que le DPO dispose d'un plan de monitoring ou de contrôle* » avant de préciser qu'un tel plan de contrôle a été établi et « *approuvé par le [Comité de direction] en sa séance du 16 septembre 2020 ».* Ce plan de contrôle a été communiqué par le contrôlé en annexe à son courrier du 16 septembre 2020.

51. 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*.[13] »

52. Il ressort du dossier d'enquête, qu'au moment de la visite sur place du 21 janvier 2019, le registre des traitements était tenu par le vice-DPD[14]. La formation restreinte relève néanmoins que cet élément pris isolément ne suffit pas à démontrer que la mission de contrôle du respect du RGPD était effectuée de manière adéquate.

53. 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

[13] WP 243 v.01, version révisée et adoptée le 5 avril 2017, p. 22
[14] Compte-rendu de la visite du 21 janvier 2019, page 2

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.* »

54. Or, tel que cela est mentionné au point 21 de la présente décision, la formation restreinte partage l'appréciation du chef d'enquête selon laquelle le contrôlé traite un nombre significatif de données personnelles.

55. 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 pouvoir démontrer que le DPD effectue sa mission de contrôle du respect du RGPD de manière adéquate.

56. La formation restreinte prend note du plan de contrôle qui a été communiqué par le contrôlé en annexe à son courrier du 16 septembre 2020.

57. Néanmoins, la formation restreinte constate que ce plan de contrôle a été établi après le début de l'enquête et considère dès lors qu'au 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.

58. 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

59. 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.* »

60. 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 ».

61. 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.

62. 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 l'imposition d'une amende administrative

63. Dans son courrier complémentaire à la communication des griefs du 10 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 23.400 euros.

64. 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 38.1 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 est associé dès le stade le plus précoce possible à toutes les questions relatives à la protection des données et exerce ses missions de façon effective, notamment 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'il a été décidé par le contrôlé, en septembre 2020, de prendre des mesures adaptées afin de faciliter l'association du DPD à toutes les questions relatives à la protection des données. Le manquement à l'article 38.1 du RGPD a donc duré dans le temps, à tout le moins entre le 25 mai 2018 et septembre 2020 ;

(2) Qu'un plan de contrôle a été communiqué à la CNPD par le contrôlé en date du 16 septembre 2020 et que ce plan a été approuvé par le Comité de direction du contrôlé à la même date. 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 16 septembre 2020 ;

- 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, à savoir des données concernant la santé.

65. 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.

66. La formation restreinte relève que si plusieurs mesures ont été décidées par le contrôlé afin de remédier aux 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 61 de la présente décision).

67. 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 38.1 et 39.1.b) du RGPD.

68. 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 38.1 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.

69. 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 13.200 euros apparaît à la fois effectif, proportionné et dissuasif, conformément aux exigences de l'article 83.1 du RGPD.

2. Quant à la prise de mesures correctrices

70. Dans son courrier complémentaire à la communication des griefs du 10 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. Plusieurs manières peuvent être envisagées pour parvenir à ce résultat:*

- fournir un support interne ou externe à votre DPD en matière de législation spécifique en protection des données à caractère personnel et de sécurité des systèmes d'information ;

- inscrire votre DPD à des formations accélérées/intensives dans les matières ci-dessus mentionnées ;

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

b) Ordonner la mise en place de mesures permettant d'associer le 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 pourrait être d'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...).

c) 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.

d) 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. »

71. Quant aux mesures correctrices proposées par le chef d'enquête sous a) et sous c) du point 70 de la présente décision, les manquements aux articles 37.5 et 38.2 du RGPD n'étant pas constitués, il n'y pas lieu d'examiner les mesures correctrices y afférentes.

72. Quant aux autres mesures correctrices proposées par le chef d'enquête et par référence au point 62 de la présente décision, la formation restreinte prend en compte les démarches effectuées par le contrôlé afin de se conformer aux dispositions des articles 38.1 et 39.1.b) du RGPD, notamment les mesures décrites dans son courrier du 16 septembre 2020. Plus particulièrement, elle prend note des faits suivants :

- En ce qui concerne la violation de l'article 38.1 du RGPD, la formation restreinte constate qu'il a été décidé par le contrôlé de prendre des mesures adaptées afin de faciliter l'association du DPD à toutes les questions relatives à la protection des données. 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) du point 70 de la présente décision.

- En ce qui concerne la violation de l'article 39.1.b) du RGPD, la formation restreinte constate qu'un plan de contrôle a été communiqué à la CNPD par le contrôlé en date du 16 septembre 2020 et que ce plan a été approuvé par le Comité de direction du contrôlé à la même date. 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 d) du point 70 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 38.1 et 39.1.b) du RGPD ;

- de prononcer à l'encontre de la Société A une amende administrative d'un montant de treize mille deux cent euros (13.200 euros) au regard de la violation des articles 38.1 et 39.1.b) du RGPD.

Ainsi décidé à Belvaux en date du 13 octobre 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.