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

Délibération n° 40FR/2021 du 27 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 10.2;

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

Considérant ce qui suit :

I. Faits et procédure

1. Vu l'impact du rôle du délégué à la protection des données (ci-après : le « DPD ») et l'importance de son intégration dans l'organisme, et considérant que les lignes directrices concernant les DPD sont disponibles depuis décembre 2016[1], soit 17 mois avant l'entrée en application du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après : le « RGPD »), la Commission nationale pour la protection des données (ci-après : la « Commission nationale » ou la « CNPD ») a décidé de lancer une campagne d'enquête thématique sur la fonction du DPD. Ainsi, 25 procédures d'audit ont été ouvertes en 2018, concernant tant le secteur privé, que le secteur public.

2. En particulier, la Commission nationale a décidé, par délibération n°[…] du 14 septembre 2018, d'ouvrir une enquête sous la forme d'audit sur la protection des données auprès de la Société A, établie à L-[…], […], et inscrite au registre de commerce et de sociétés sous le numéro […] (ci-après, le « contrôlé ») et de désigner Monsieur 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. Le contrôlé a pour objet social l'exploitation d'une entreprise de transports […].[2] En 2018, le contrôlé occupait environ […] employés et prestait ses services auprès d'environ […] [personnes] par an.[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 courrier du 1er octobre 2018. Une visite sur place a eu lieu le 20 février 2019. Suite à ces échanges, le chef d'enquête a établi le rapport d'audit n° […] (ci-après : le « rapport d'audit »).

[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.

[2] Objet social tel que déclaré au Registre de commerce et des sociétés du Luxembourg, article 2.1 des statuts coordonnés au […] du contrôlé.

[3] Compte-rendu de la visite sur place du 20 février 2019.

5. Il ressort du rapport d'audit qu'afin de vérifier la conformité du contrôlé 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'intérêts ;
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 30 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. La rapport d'audit était joint audit courrier du 30 octobre 2019.

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

- l'obligation d'associer le DPD à toutes les questions relatives à la protection des données à caractère personnel[4] ;

[4] Objectif 8

- l'obligation de garantir l'autonomie du DPD[5] ;
- les missions d'information et de conseil du DPD[6] ;
- la mission de contrôle du DPD[7].

8. Le 3 août 2020, le chef d'enquête a adressé au contrôlé un courrier complémentaire à la communication des griefs (ci-après : le « courrier complémentaire à la communication des griefs ») par lequel il informe le contrôlé des mesures correctrices que le chef d'enquête propose à la Commission nationale siégeant en formation restreinte (ci-après : la « formation restreinte ») d'adopter.

9. Par courriers des 12 décembre 2019 et 14 octobre 2020, le contrôlé a fait parvenir au chef d'enquête sa prise de position quant à la communication des griefs et au courrier complémentaire à la communication des griefs. Dans ces courriers, le contrôlé présente ses observations relatives à chaque manquement soulevé par le chef d'enquête dans la communication des griefs et conteste la proposition d'amende administrative, « *les manquements décrits relevant davantage du formalisme que d'un non-exercice des rôles et missions du DPD* ».

10. La présidente de la formation restreinte a informé le contrôlé par courrier du 12 avril 2021 que son affaire serait inscrite à la séance de la formation restreinte du 16 juin 2021 et qu'il pouvait assister à cette séance. Le contrôlé a informé par courriel du 12 mai 2021 qu'il participerait à ladite séance.

11. Lors de la séance de la formation restreinte du 16 juin 2021, le chef d'enquête et le contrôlé ont présenté leurs observations orales sur l'affaire et ont répondu aux questions posées par la formation restreinte. Le contrôlé a eu la parole en dernier.

12. Le contrôlé a fourni des informations complémentaires par courrier du 29 juin 2021, suite à une demande en ce sens de la formation restreinte.

[5] Objectif 7
[6] Objectif 9
[7] Objectif 10

II. En droit

A. 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

13. 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.

14. 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* »[8].

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

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

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

16. En outre, 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 traitements dans lesquels le DPD doit être consulté.

2. <u>En l'espèce</u>

17. 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.

18. Selon la communication des griefs, page 2, le DPD du contrôlé participe au Comité de Direction en fonction de l'ordre du jour (en l'occurrence aux Comités de Direction des 30 mai 2018, 1er août 2018 et 5 février 2019) ainsi qu'aux réunions de gestion de projet. Aucune règle ou fréquence n'a été définie de façon formelle quant à la participation du DPD à ces comités ou réunions.

19. Dans sa prise de position du 12 décembre 2019, le contrôlé a indiqué que, à partir du 1er janvier 2020, un rapport trimestriel d'activité en matière de protection des données personnelles sera présenté au Comité de Direction, dans les 2 semaines suivant la fin de chaque trimestre considéré.

20. Dans sa prise de position du 14 octobre 2020, le contrôlé a ajouté que, depuis la nomination du DPD le 15 mai 2018, celui-ci participe aux Comités de Direction de façon régulière. En outre, les rapports d'activités du DPD ont été présentés au Comité de Direction à 6 reprises entre mai 2018 et décembre 2019, soit une fréquence trimestrielle. Cette fréquence de présentation du rapport d'activité a été formalisée comme indiquée dans le courrier du 12 décembre 2019. Selon le contrôlé, il s'agit donc d'une simple formalisation d'une pratique déjà en place.

21. En outre, le contrôlé indique que le DPD peut être consulté ad hoc, par le Comité de Direction dès qu'une question relative au traitement des données à caractère personnel se pose.

« *Cette possibilité a été activée à plusieurs reprises au cours des deux dernières années (2018-2020) et surtout ces derniers mois dans le cadre des mesures mises en place dans la lutte contre le Covid-19 : le DPD a notamment participé aux Comités de Direction des 21 juillet 2020 et 22 septembre 2020* ».

22. Le contrôlé explique également que le DPD est associé à la conception de nouveaux projets et à la mise en œuvre de nouvelles solutions informatiques de la façon suivante :

- le DPD est contacté systématiquement dès qu'un nouveau projet ou produit est lancé. « *La méthodologie projet impose en effet une étape d'analyse et de validation ente le DPD et le département initiateur ou gestionnaire de la nouvelle idée à mettre en œuvre* ».
- « *En cas de sélection d'un fournisseur de services externes pour la sélection d'une nouvelle solution informatique ou pour externaliser un processus de gestion de données (peu importe la typologie de données échangées), le DPD est partie prenante à l'évaluation du fournisseur de services concerné*. »
- « *Les réunions de gestion du portefeuille de projets [du contrôlé] se tiennent quant à elles sur une base mensuelle et le DPD est une fonction systématiquement présente non seulement pour prendre connaissance des idées nouvelles qui pourraient émerger dans les différents départements avant que ces dernières ne deviennent des projets. Cette étape permet d'alerter éventuellement sur les risques de conformité à prendre en compte très en amont des initiatives.* »

23. Dans son courrier du 29 juin 2021, le contrôlé informe également la formation restreinte que le DPD doit approuver chaque demande relative à un transfert de données personnelles aux autorités locales et étrangères, conforment à la politique de transfert de données personnelles aux autorités locales et étrangères mise en place en mai 2018.

24. La formation restreinte prend note de la mise en place par le contrôlé d'une formalisation de l'implication du DPD auprès du Comité de Direction. Si cette mesure de formalisation devrait faciliter l'association du DPD à toutes les questions relatives à la protection des données, il convient néanmoins de constater que celle-ci a été décidée en cours d'enquête.

25. En outre, le contrôlé n'a pas apporté la preuve quant à la présentation du rapport d'activités du DPD au Comité de Direction sur une fréquence trimestrielle entre mai 2018 et décembre 2019. En effet, dans sa prise de position du 14 octobre 2020, le contrôlé soutient qu'un rapport d'activité est présenté au Comité de Direction sur une fréquence trimestrielle mais, au regard des pièces transmises en annexe de ce courrier, le contrôlé n'apporte la preuve que pour la présentation faite devant le Comité de Direction au mois de décembre 2019.

26. La formation restreinte se rallie par conséquent au constat du chef d'enquête selon lequel, au début de l'enquête, le responsable du 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 à caractère personnel.

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

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

1. Sur les principes

28. 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.

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

30. Selon les lignes directrices concernant les DPD[9], 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,*

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

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. A cet égard, l'article 38, paragraphe 3, dispose que le DPD « fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant ». Une telle reddition de compte directe garantit que l'encadrement supérieur (par ex., le conseil d'administration) a connaissance des avis et recommandations du DPD qui s'inscrivent dans le cadre de la mission de ce dernier consistant à informer et à conseiller le responsable du traitement ou le sous-traitant. L'élaboration d'un rapport annuel sur les activités du DPD destiné au niveau le plus élevé de la direction constitue un autre exemple de reddition de compte directe. »

2. <u>En l'espèce</u>

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

32. Selon la communication des griefs, page 3, « *[l]ors de l'enquête, les agents de la CNPD ont constaté que le DPD est rattaché hiérarchiquement au Département « Risk Management et Audit Interne ». Ce département est rattaché aux Services Généraux, qui dépendent eux-mêmes de la Direction. Il y a donc deux niveaux hiérarchiques entre le DPD et la Direction. Bien que le DPD soit fonctionnellement rattaché à la Direction et qu'il participe au Comité de Direction en fonction de l'ordre du jour, le rattachement hiérarchique à la Direction et donc l'accès direct et permanent à cette dernière n'est pas formellement garanti.* »

33. Dans ses prises de position des 12 décembre 2019 et 14 octobre 2020, le contrôlé indique que « *[l]a garantie de l'autonomie du DPD, et l'accès direct à la Direction Générale, qui étaient déjà une réalité pratique au moment de [l']audit, ont été renforcés et matérialisés dans l'organigramme de la compagnie. Le DPD est désormais directement rattaché à la Direction des*

Services Généraux, et non plus au département Risk Management et Audit Interne. » Un nouvel organigramme a été publié le 11 décembre 2019 afin de refléter ce changement.

34. 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 relève néanmoins 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* ».

35. Or, 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 significatif de données personnelles* ».

36. La formation restreinte considère que le contrôlé n'a pas démontré la mise en place d'autres mesures qui permettraient de démontrer que le DPD est en mesure d'accéder directement au plus haut niveau de la direction dès qu'il l'estime nécessaire, sans devoir obligatoirement passer par les niveaux hiérarchiques intermédiaires. Dès lors, 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.

37. 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 du 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.

38. 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.

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

1. Sur les principes

39. 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 Etats membres en matière de protection des données* ».

2. En l'espèce

40. 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* ».

41. Selon la communication des griefs, page 3, « *[i]l ressort de l'enquête que l'organisme n'a pas de reporting d'activité spécifique sur la protection des données destiné à l'encadrement supérieur (Comité de Direction, Conseil d'Administration). Bien que des points réguliers soient réalisés au Comité de Direction concernant les problématiques liées à la protection des données et que toutes les procédures relatives à la protection des données sont soumises à la Direction pour validation, ces éléments ne sauraient compenser l'absence de reporting formel des activités du DPD vers le Comité de Direction sur base d'une fréquence définie* ».

42. Dans sa prise de position du 12 décembre 2019, le contrôlé fait savoir que le DPD « *effectue des points réguliers au Comité de Direction sur son activité, sans que la périodicité de ce reporting ait été définie de manière formelle. A partir du 1er janvier 2020, un rapport trimestriel d'activité en matière de protection des données sera présenté au Comité de Direction, dans les 2 semaines suivant la fin de chaque trimestre considéré.* »

43. Dans sa prise de position du 14 octobre 2020, le contrôlé indique également que « *[l]a notion de reporting régulier auprès de la Direction Générale était déjà présente dans l'amendement du contrat du DPD, sur une base bi-annuelle. Cette fréquence de reporting a été relevée et portée à 4 fois par an* ». Cet avenant au contrat du DPD a cependant été signé le 31 mars 2020, soit après le début de l'enquête.

44. 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 mises 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 du 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* ».

45. Il ressort du dossier d'enquête que le DPD soumet des points réguliers relatifs à la protection des données au Comité de Direction. Le DPD a par exemple présenté en février 2019 un suivi de la conformité au RGPD au 31 décembre 2018 et, en août 2018, une étude sur le consentement et la problématique de conservation des données. Cependant, il n'y a pas de reporting d'activité spécifique, sur base d'une fréquence définie.[10]

46. Néanmoins la formation restreinte rappelle qu'elle a déjà constaté au point 34 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 du traitement au regard de la sensibilité des données traitées et des risques encourus par les personnes concernées* ».

[10] Compte rendu de visite du 20 février 2019, p. 4, et rapport d'audit, p.8

47. Or, tel que cela est mentionné au point 35 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 significatif de données personnelles* ». La formation restreinte considère dès lors qu'un reporting formel des activités du DPD auprès de la direction, sur 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.

48. La formation restreinte prend note du fait que le contrôlé a indiqué dans ses courriers des 12 décembre 2019 et 14 octobre 2020 qu'il a été décidé de mettre en place un reporting formel des activités du DPD sur une base trimestrielle. 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 du 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 du traitement.

49. 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.

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

1. Sur les principes

50. 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 Etats 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* ».

51. Le considérant (97) précise que le DPD devrait aider l'organisme à vérifier le respect, au niveau interne, du RGPD.

52. Il résulte des lignes directrices concernant les DPD[11] 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. <u>En l'espèce</u>

53. 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)* ».

54. Selon la communication des griefs, page 3, « *[i]l ressort de l'enquête que l'organisme ne dispose pas de plan de contrôle formalisé, spécifique à la protection des données. La CNPD prend bonne note qu'une revue annuelle en matière de protection des données est prévue par le département légal ainsi qu'une revue régulière du registre des traitements. La CNPD note également qu'un Compliance Officer qui aura dans ses attributions la revue régulière de la conformité en matière de protection des données est en cours de recrutement et que des missions de contrôle relatives à la protection des données seront intégrées au plan d'audit interne. Néanmoins, l'organisme n'effectuait pas les missions de contrôle au moment de l'enquête.* »

55. Dans sa prise de position du 12 décembre 2019, le contrôlé indique qu'un Compliance Officer directement rattaché à la Direction des Services Généraux a été nommé, avec dans ses attributions la revue régulière de la conformité en matière de protection des données.

56. Dans sa prise de position du 14 octobre 2020, le contrôlé présente les contrôles qui ont été réalisés et documentés par le DPD :

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

- Pour chaque nouveau projet et produit, le DPD revoit le processus, documente le niveau de risque et revoit en collaboration avec le département légal les documents contractuels.
- Une revue contractuelle est effectuée de manière annuelle avec le département légal depuis la création de la fonction de DPD.
- Un projet de vérification des procédures de conservation des données a été effectué en 2019 avec l'aide d'un consultant externe sous la supervision du DPD. Les conclusions de cette étude ont été présentées lors du rapport d'activités du DPD en décembre 2019.
- Le DPD s'est saisi à plusieurs reprises de contrôles ad-hoc suite à des demandes d'information de personnes concernées.
- En décembre 2019, le contrôlé a mandaté son réviseur des comptes pour conduire une revue des procédures « Data Protection Office » et des contrôles en place afin d'évaluer les risques GDPR associés. Le DPD était partie prenante de cette revue.

57. Dans son courrier du 29 juin 2021, le contrôlé ajoute que […] « Data Protection Coordinators » ont été nommés en mai 2018 afin de contrôler la conformité des pratiques commerciales avec les exigences du RGPD et reporter au DPD. Ces Data Protection Coordinators ont reçu des formations en juin et juillet 2018 ainsi qu'en février et mars 2021.

58. Le contrôlé indique également la mise en place de réunions biannuelles entre le DPD et le Directeur général afin de discuter des projets de contrôle à venir. Ces réunions biannuelles sont mentionnées dans l'avenant au contrat du DPD signé le 31 mars 2020, tel que mentionné au point 43 de la présente décision.

59. 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 « *ce 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 et du sous-traitant[12] ».

60. En outre, la formation restreinte rappelle qu'elle a déjà constaté au point 34 de la présente décision qu'il est précisé à juste titre en page 2 de la communication des griefs (sous « remarques préliminaires ») que « *les 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 du traitement au regard de la sensibilité des données traitées et des risques encourus par les personnes concernées* ».

61. Or, tel que mentionné au point 35 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 significatif de données personnelles.

62. La formation restreinte comprend que le contrôlé a mis en place plusieurs mesures afin de renforcer les capacités du DPD à effectuer sa mission de contrôle du respect du RGPD, telle que la nomination d'un Compliance Officer et la mise en place de réunions biannuelles entre le DPD et le Directeur Général. Cependant, ces mesures ont été prises en cours d'enquête.

63. Compte tenu du fait que les activités du contrôlé impliquent des traitements de données à caractère personnel qui touchent un nombre important de personnes concernées, la formation restreinte considère que la mission de contrôle effectuée par le DPD auprès du contrôlé doit être formalisée, par exemple par un plan de contrôle en matière de protection des données, afin de pouvoir démontrer que le DPD puisse effectuer sa mission de contrôle du respect du RGPD de façon adéquate.

64. Par conséquent, la formation restreinte est d'avis que le contrôlé n'a pas été en mesure de démontrer que, au début de l'enquête, le DPD pouvait exercer sa mission de contrôle de la conformité du responsable du traitement au RGPD.

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

65. 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

66. 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.* »

67. 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 des 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* ».

68. 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.

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

B. <u>En l'espèce</u>

1. <u>Quant à l'imposition d'une amende administrative</u>

70. Dans son courrier complémentaire à la communication des griefs du 3 août 2020, le chef d'enquête propose à la formation restreinte de prononcer à l'encontre du contrôlé une amende administrative portant sur le montant de 15.400 euros.

71. 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, 38.3, 39.1 a) et 39.1 b) du RGPD, la formation restreinte relève que la nomination d'un DPD par un organisme ne saurait être efficiente et efficace, à savoir faciliter le respect du RGPD par l'organisme, que dans le cas où le DPD est associé à toutes les questions relatives à la protection des données, puisse exercer sa fonction en toute autonomie, et puisse exercer de façon effective ses missions, dont la mission d'information et de conseil du responsable du traitement et la mission de contrôle du respect du RGPD.

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

(1) Le contrôlé a informé la CNPD, dans ses prises de positions des 12 décembre 2019, 14 octobre 2020 et 21 juin 2021, de la formalisation de l'association du DPD aux questions relatives à la protection des données. Ces mesures ont néanmoins été

décidées en cours d'enquête. A titre d'exemple, selon les informations à la disposition de la formation restreinte, la formalisation du reporting des activités du DPD sur une fréquence trimestrielle aurait été mise en place en date du 1er janvier 2020 (prise de position du contrôlé du 12 décembre 2019) alors que, dans l'avenant au contrat du DPD signé le 31 mars 2020 (annexé à la prise de position du contrôlé du 14 octobre 2020), la fréquence du reporting est mentionnée comme étant biannuelle. Le manquement à l'article 38.1 du RGPD a donc duré dans le temps, à tout le moins du 25 mai 2018 au 1er janvier 2020.

(2) Dans ses prises de position des 12 décembre 2019 et 14 octobre 2020, le contrôlé a informé la CNPD d'un changement dans l'organigramme de l'organisme, publié le 11 décembre 2019, de façon à ce que le DPD soit désormais rattaché directement à la Direction des Services Généraux. Le manquement à l'article 38.3 du RGPD a donc duré dans le temps, à tout le moins du 25 mai 2018 au 11 décembre 2019.

(3) Il n'a pas été démontré par le contrôlé que, au moment de l'ouverture de l'enquête, le DPD exerçait ses missions d'information et de conseil à l'égard du responsable du traitement. Comme relevé au point (1) ci-dessus et au point 48 de la présente décision, un reporting des activités du DPD sur une fréquence trimestrielle aurait été mise en place en date du 1er janvier 2020, alors que dans l'avenant au contrat de travail du DPD signé le 31 mars 2020, la fréquence du reporting est mentionnée comme étant biannuelle. La formation restreinte comprend donc qu'un reporting par le DPD à la direction du contrôlé a été mis en place, bien que la fréquence de ce reporting ne soit pas clarifiée. Le manquement à l'article 39.1 a) a donc duré dans le temps, à tout le moins du 25 mai 2018 au 1er janvier 2020.

(4) Il n'a pas été démontré que le DPD remplissait sa mission de contrôle du respect du RGPD par le contrôlé au début de l'enquête. Le contrôlé a informé la CNPD de la nomination d'un Compliance Officer en charge de ce contrôle, sans indiquer toutefois la date de cette nomination. En outre, le contrôlé a indiqué la mise en place de réunions biannuelles entre le DPD et le Directeur général, tel que cela est prévu dans l'avenant au contrat du DPD signé le 31 mars 2020 et déjà mentionné aux points 43

et 58 de la présente décision. Ces mesures ont néanmoins été décidées en cours d'enquête et la formation restreinte ne dispose pas de la documentation nécessaire permettant de constater que le manquement a pris fin. Le manquement à l'article 39.1 b) du RGPD a donc duré dans le temps, à partir du 25 mai 2018.

- Quant au critère à prendre en compte relatif au nombre de personnes concernées, le cas échéant, affectées par la violation et le niveau de dommage, le cas échéant, subi [article 83.2 a) du RGPD], la formation restreinte relève que le contrôlé compte environ […] employés et […] de [personnes] par an.

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

72. 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.

73. La formation restreinte relève que si plusieurs mesures ont été décidées par le contrôlé afin de remédier en totalité ou en partie à certains manquements, celle-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 68 de la présente décision).

74. 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 manquements aux articles 38.1, 38.3, 39.1 a) et 39.1 b) du RGPD.

75. 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, 38.3, 39.1 a) et 39.1 b) du RGPD est reproché au contrôlé, le montant maximum de l'amende pouvant être retenu s'élève à 10 millions d'euros ou 2% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

76. 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 15.400 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

77. 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 assurant une association 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 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 avec l'agenda des réunions, invitation, fréquence, statut de membre permanent, etc....).*

b) Ordonner la mise en place de mesures garantissant l'autonomie du DPD conformément aux exigences de l'article 38 paragraphe 3 du RGPD. Plusieurs mesures peuvent être envisagées pour parvenir à ce résultat, telles que le rattachement du DPD au plus haut niveau de la direction afin de garantir au maximum son autonomie ou la création d'une ligne formalisée et régulière de reporting direct, ainsi qu'un mécanisme d'escalade d'urgence à la direction permettant de contourner le(s) niveau(x) hiérarchique(s) intermédiaire(s).

c) Ordonner la mise en place de mesures permettant au DPD d'informer et de conseiller le responsable du 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) Ordonner le déploiement de la mission de contrôle, conformément à l'article 39 paragraphe 1 b) du RGPD. Le DPD devrait ainsi documenter ses contrôles relatifs à 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. Il est à rappeler que l'exécution de ces contrôles est du ressort du DPD, qui doit toujours contrôler et superviser les travaux réalisés en cas de délégation. »

78. Quant aux mesures correctrices proposées par le chef d'enquête et par référence au point 69 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, 38.3, 39.1 a) et 39.1 b) du RGPD, notamment les mesures décrites dans ses courriers des 12 décembre 2019, 14 octobre 2020 et 26 juin 2021. 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 que le contrôlé a formalisé l'association du DPD aux questions relatives à la protection des données en définissant une fréquence spécifique de participation du DPD au Comité de Direction. La formation restreinte considère dès lors qu'il n'y a pas lieu de prononcer la mesure correctrice proposée par le chef d'enquête et reprise sous a) du point 77 de la présente décision.

- En ce qui concerne la violation de l'article 38.3 du RGPD, la formation restreinte constate que le contrôlé a opéré un changement dans l'organigramme de l'organisme, publié le 11 décembre 2019, de façon à ce que le DPD soit désormais rattaché directement à la Direction des Services Généraux. La formation restreinte considère dès lors qu'il n'y a pas lieu de prononcer la mesure correctrice proposée par le chef d'enquête et reprise sous b) du point 77 de la présente décision.

- En ce qui concerne la violation de l'article 39.1 a) du RGPD, la formation restreinte comprend que le contrôlé a mis en place un reporting des activités du DPD au Comité de Direction sur base d'une fréquence spécifique (fréquence trimestrielle ou biannuelle). La formation restreinte considère dès lors qu'il n'y a pas lieu de prononcer la mesure

correctrice proposée par le chef d'enquête et reprise sous c) du point 77 de la présente décision.

- En ce qui concerne la violation de l'article 39.1 b) du RGPD, la formation restreinte est d'avis qu'elle ne dispose pas de la documentation nécessaire pour déterminer avec suffisance l'exercice par le DPD de sa mission de contrôle de la conformité du contrôlé au RGPD. La formation restreinte considère dès lors qu'il y a lieu de prononcer la mesure correctrice proposée par le chef d'enquête et reprise sous d) du point 77 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, 38.3, 39.1 a) et 39.1 b) du RGPD ;

- de prononcer à l'encontre de la Société A une amende administrative d'un montant de quinze mille quatre cent euros (15.400 euros) au regard de la violation des articles 38.1, 38.3, 39.1 a) et 39.1 b) du RGPD ;

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

  s'assurer que le DPD puisse exercer sa mission de contrôle de la conformité du responsable du traitement au RGPD.

Ainsi décidé à Belvaux en date du 27 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.