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

Délibération n° 18FR/2021 du 31 mai 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 et ayant son siège social à L- […], inscrite au registre de commerce et des 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 notamment pour objet […][2]. Le contrôlé compte environ […] employés répartis sur […] sites ainsi que […][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 5 octobre 2018. Une visite sur place a eu lieu le 21 janvier 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] Statuts coordonnés déposés le […].
[3] Présentation du contrôlé du 21 janvier 2019

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

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

- l'obligation d'associer le DPD à toutes les questions relatives à la protection des données à caractère personnel[4] ;
- l'obligation de fournir les ressources nécessaires au DPD[5] ;
- la mission d'information et de conseil du DPD[6].

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

8. Par courrier du 22 novembre 2019, le contrôlé a adressé au chef d'enquête sa prise de position quant aux manquements énumérés dans la communication des griefs.

9. Le 24 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 et l'amende administrative qu'il propose à la Commission nationale siégeant en formation restreinte (ci-après : la « formation restreinte ») d'adopter.

10. Par courrier du 30 septembre 2020, le contrôlé a fait parvenir au chef d'enquête ses observations quant au courrier complémentaire à la communication des griefs.

11. L'affaire a été à l'ordre du jour de la séance de la formation restreinte du 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 exposé leurs observations orales à l'appui de leurs observations écrites. Plus particulièrement, Maître […], mandataire du contrôlé, a donné lecture d'une note exposant les observations du contrôlé (ci-après : la « note de plaidoiries »). Le chef d'enquête et le contrôlé ont par la suite répondu aux questions posées par la formation restreinte. Le contrôlé a eu la parole en dernier.

12. Par courriel du 27 janvier 2021, le mandataire du contrôlé a transmis à la formation restreinte une copie de la note de plaidoiries, un extrait d'une présentation datée du 8 octobre 2018 présentant l'organigramme « Data Protection » avec indication du « [Comité GDPR] » du contrôlé ainsi qu'un extrait du registre de commerce et des sociétés de la […] Société B gérant […] à Luxembourg.

II. En droit

A. Quant aux exigences de précision de la communication des griefs et du courrier complémentaire à la communication des griefs

13. Dans sa note de plaidoiries, le mandataire du contrôlé invoque, à titre liminaire, que la communication des griefs et le courrier complémentaire à la communication des griefs manquent de précision :

« *[…] les Courriers de Grief manquent aux obligations légales applicables en matière administrative, notamment en ce qu'ils ne contiennent pas de référence précise à une norme juridique qui aurait été violée et qu'ils ne contiennent aucune indication précise des faits détaillés qui seraient constitutifs d'une violation d'une norme juridique par Société A. Par ce manque de précision, les principes généraux de droits applicables ont été violés et ma mandante a été privée de la possibilité de fournir des explications éclairées et détaillées susceptibles d'éclairer la Formation Restreinte.* »

14. La formation restreinte constate que le chef d'enquête mentionne expressément, tant dans la communication des griefs que dans le courrier complémentaire à la communication des griefs, les dispositions du RGPD auxquelles le contrôlé aurait manqué, à savoir les articles 38.1, 38.2 et 39.1. a). Par ailleurs, les constats factuels faits lors de l'enquête et sur lesquels les manquements allégués sont basés sont indiqués dans la communication des griefs. De surplus, le rapport d'audit reprenant l'ensemble des constats et travaux effectués par le chef d'enquête dans le cadre de la mission d'audit était joint à la communication des griefs. En outre, la formation restreinte note que le mandataire du contrôlé fait référence aux « *obligations légales applicables en matière administrative* » ainsi qu'aux « *principes généraux de droits applicables* » sans pour autant préciser quelle règle de droit aurait été violée en l'espèce.

15. A toutes fins utiles, il y a lieu de constater que le contrôlé était en mesure de prendre position par rapport aux manquements lui reprochés, comme le démontre ses prises de position des 22 novembre 2019 et 30 septembre 2020 ainsi que les observations orales et la note de plaidoiries présentées à la séance de la formation restreinte du 26 janvier 2021.

16. C'est partant à tort que le mandataire du contrôlé soutient que la communication des griefs et le courrier complémentaire à la communication des griefs manquent de précision de sorte que sa mandante aurait été « *privée de la possibilité de fournir des explications éclairées et détaillées susceptibles d'éclairer la Formation Restreinte* ».

B. <u>Quant aux griefs énumérés dans la communication des griefs</u>

a) <u>Sur le manquement à l'obligation d'associer le DPD à toutes les questions relatives à la protection des données à caractère personnel</u>

1. Sur les principes

17. 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.

18. 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* »[7].

19. 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.

20. 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.

2. En l'espèce

21. Il ressort du rapport d'audit que, pour que le chef d'enquête considère l'objectif 8 comme atteint par le contrôlé dans le cadre de cette campagne d'audit, le chef d'enquête

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

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.

22. Selon la communication des griefs, page 3, « *le DPD participe à de nombreuses réunions au niveau Groupe et […] organise régulièrement des réunions avec ses points de contacts locaux. Mais ces éléments ne suffisent pas à démontrer le caractère direct, formel et permanent de l'implication du DPD à Luxembourg* ». Il résulte encore de la communication des griefs que « *le DPD Groupe reçoit un rapport mensuel de la part du point de contact local suite au […] ainsi qu'un reporting mensuel […] relatif aux problématiques de protection des données (nombre de demandes d'exercice de droits ou de réclamations, analyses d'impact éventuelles etc.). […] le DPD est informé et consulté systématiquement par le point de contact local en cas d'incident de sécurité étant susceptible d'impliquer des données à caractère personnel et de créer un risque pour les personnes concernées.* » Le chef d'enquête estime toutefois que *« ces éléments ne sauraient compenser l'absence d'une implication directe du DPD Groupe au sein de la Société A, ce qui pourrait engendrer le risque que le DPD ne soit pas suffisamment impliqué au niveau opérationnel à Luxembourg*. » Finalement, le chef d'enquête fait valoir qu'il « *n'a pas eu connaissance d'éléments permettant d'adresser ce risque, comme par exemple la mise en place formelle de visites sur base d'une fréquence définie du DPD Groupe (ou d'un membre de son équipe Data Protection) à Luxembourg. Ces visites permettraient notamment au DPD de pouvoir discuter directement avec l'encadrement supérieur de la Société A des problématiques liées à la protection des données et de pouvoir évaluer directement les problématiques opérationnelles.* »

23. Dans sa prise de position du 22 novembre 2019, le contrôlé affirme que le DPD Groupe est associé d'une manière appropriée et en temps utile à toutes les questions relatives à la protection des données à caractère personnel. Le contrôlé expose que « *[t]outes les questions relatives à la protection des données personnelles initiées au Grand-Duché de Luxembourg sont réceptionnées et analysées dans un premier temps par notre point de contact dédié à la protection des données au Luxembourg* » (ci-après : le « point de contact local ») et que ce dernier travaille en étroite collaboration avec le DPD Groupe […]. Selon le contrôlé, le point de contact est chargé de la gestion de conformité des traitements de données à caractère personnel mis en œuvre par le contrôlé, cela sous la supervision du DPD Groupe à qui le point de contact rapporte ses actions. Par ailleurs, le contrôlé mentionne dans sa prise de position

du 22 novembre 2019 l'institution d'un comité dédié à la protection des données à Luxembourg (ci-après : le « [Comité GDPR] ») qui définit la stratégie sur ces sujets et les plans d'actions associés. Le contrôlé expose la composition et le fonctionnement du [Comité GDPR] pour soutenir que le DPD Groupe est impliqué dans la gestion de la conformité avec les dispositions du RGPD au Luxembourg.

24. Dans sa note de plaidoiries, le mandataire du contrôlé met en avant l'article 37.2 du RGPD, qui autorise un groupe d'entreprises à désigner un seul DPD à condition que ce dernier soit facilement joignable à partir de chaque lieu d'établissement, ainsi que les lignes directrices concernant les DPD pour soutenir que le fonctionnement du contrôlé est conforme au RGPD et affirme que *« [i]l n'a été constaté aucune matérialité des faits reprochés, aucune indisponibilité du DPD de la Société A que ce soit vis-à-vis de l'autorité de contrôle ou encore des personnes concernées et un risque éventuel et non caractérisé ne saurait permettre d'établir factuellement une violation*. »

25. La formation restreinte prend note que le contrôlé est une filiale du groupe […] et que ce dernier avait décidé de désigner un seul DPD pour les différentes entités du groupe (ci-après : le « DPD Groupe »). Au niveau central, le groupe a mis en place un bureau de la protection des données *(« […] »)* composé du DPD Groupe ainsi que de […] juristes spécialisés en matière de protection des données et […] *project manager.* Au niveau local, l'unique juriste du contrôlé a été désigné comme point de contact local du DPD Groupe.

26. A titre liminaire, la formation restreinte constate que le manquement allégué par le chef d'enquête a trait à l'article 38.1 du RGPD de sorte que les explications du mandataire du contrôlé concernant l'article 37.2 du RGPD ne sont pas pertinentes en l'espèce. En effet, même si le RGPD autorise un groupe d'entreprises à désigner un seul DPD, il n'en demeure pas moins que ce DPD doit être associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel, conformément à l'article 38.1 du RGPD. Il est ainsi loisible à un organisme de désigner un seul DPD au niveau du groupe dont les entités sont établies dans plusieurs Etats membres de l'Union européenne et de prévoir, au niveau local, des « points de contact » qui assistent le DPD notamment dans les questions relatives aux particularités locales telles que la législation nationale. Dans un tel cas de figure, il est toutefois d'autant plus important de définir clairement, entre autres, les modalités de collaboration entre le DPD et les « points de contact locaux » ainsi que la répartition des tâches et responsabilités.

En l'espèce, la formation restreinte note que toutes les questions relatives à la protection des données à caractère personnel qui se posaient au niveau du contrôlé étaient réceptionnées et analysées dans un premier temps par le point de contact local qui s'adressait au DPD Groupe lorsqu'il l'estimait nécessaire. La formation restreinte note encore que le DPD Groupe ne faisait pas partie du [Comité GDPR] et n'était informé des sujets y discutés qu'à travers les procès-verbaux du [Comité GDPR] et par l'intermédiaire des questions soulevées par le point de contact local lors de ces réunions.

27. Il ressort partant du dossier d'enquête que le DPD Groupe n'était associé qu'indirectement aux questions relatives à la protection des données à caractère personnel qui se posaient au niveau du contrôlé, cela par l'intermédiaire du point de contact local qui, dans les faits, agissait en tant qu'interlocuteur en matière de protection des données au sein de l'organisme. Or, le point de contact local était l'unique juriste du contrôlé et ne faisait pas partie de l'équipe du DPD Groupe à proprement parler, à savoir le bureau de la protection des données (« *[…]* »).

28. Par ailleurs, la formation restreinte estime que le fait de transmettre les procès-verbaux du [Comité GDPR] au DPD Groupe ne permet pas d'établir son association appropriée et en temps utile dans la mesure où le DPD Groupe est simplement informé des mesures que le [Comité GDPR] propose aux différents organes décisionnels du contrôlé de mettre en œuvre. Le DPD n'est donc pas informé et surtout pas consulté « *dès le stade le plus précoce possible* » de toutes les questions relatives à la protection des données.

29. En outre, le contrôlé indique dans sa prise de position du 30 septembre 2020 que le point de contact local a été désigné comme DPD pour la Société A, avec effet au 1er octobre 2020. La formation restreinte constate que la CNPD a reçu la déclaration modificative par courriel du 30 septembre 2020. Or, le contrôlé doit veiller à ce que le DPD nouvellement nommé soit effectivement associé à toutes les questions relatives à la protection des données à caractère personnel. Le fait d'avoir nommé le point de contact local comme DPD ne suffit pas à démontrer à suffisance une telle association de ce dernier à toutes les questions relatives à la protection des données à caractère personnel.

30. Au vu de ce qui précède, la formation restreinte se rallie au constat du chef d'enquête selon lequel la non-conformité à l'article 38.1 du RGPD était acquise au moment de l'enquête.

b) Sur le manquement à l'obligation de fournir les ressources nécessaires au DPD

1. Sur les principes

31. 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.* »

32. Il résulte des lignes directrices concernant les DPD que les aspects suivants doivent notamment être pris en considération[8] :

- « *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* ».

33. 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.* »

2. En l'espèce

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

34. Il ressort du rapport d'audit que, au vu de la taille des organismes sélectionnés, pour que le chef d'enquête considère l'objectif 6 comme atteint par le contrôlé dans le cadre de cette campagne d'audit, le chef d'enquête s'attend à ce que le contrôlé emploie 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.

Il résulte de la communication des griefs, page 3, que le DPD Groupe dispose au niveau central d'une équipe composée de […] juristes spécialisés en matière de protection des données ainsi que […] *project manager*. Au niveau local, le DPD Groupe ne dispose toutefois que d'un point de contact local qui était par ailleurs l'unique juriste du contrôlé de sorte que le chef d'enquête relève « *le risque que le DPD n'ait pas suffisamment de ressources au niveau local à Luxembourg, les ressources étant concentrées au niveau du groupe, mais ne semblant pas suffisamment déployées au niveau local* » ainsi que *« le risque qu'en cas de fort pic d'activité concernant les affaires juridiques à traiter au sein de la Société A, le point de contact local ne puisse pas avoir les moyens de s'acquitter efficacement de ses missions relatives à la protection des données, ce qui engendrerait le risque que le DPD ne puisse pas exercer efficacement ses missions de DPD pour le Luxembourg* ».

35. Dans sa prise de position du 22 novembre 2019, le contrôlé affirme que le DPD Groupe dispose au niveau local du soutien d'une équipe juridique composée du point de contact local et d'une « *seconde ressource* » et note que « *la description de poste du Point de Contact Local et de la deuxième ressource dans l'équipe juridique locale en contrat à durée indéterminée doit être détaillée en termes de volume horaire et de description des tâches* ».

36. Dans sa note de plaidoiries, le mandataire du contrôlé fait par ailleurs valoir que l'exigence de formaliser la répartition du temps de travail n'existe pas dans la règlementation applicable et que les lignes directrices concernant les DPD contiennent tout au plus une recommandation à titre 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* ». Finalement, le mandataire du contrôlé soutient qu' « *[i]l n'a, ici non plus, été constaté aucune matérialité des faits reprochés, ni fourni aucune explication sur les critères examinés pour conclure à un manque de ressources, ni aucune analyse des ressources existantes. Un risque éventuel et non caractérisé ne saurait*

permettre d'établir factuellement que la Société A manquerait de ressources pour faire face à ses obligations au titre de la protection des données. »

37. La formation restreinte prend note que le contrôlé a opté pour désigner le DPD Groupe qui dispose, au niveau central, d'une équipe composée de […] juristes spécialisés en matière de protection des données ainsi que […] *project manager*. Au niveau de l'entité luxembourgeoise ayant fait l'objet de l'enquête, un point de contact local a été nommé, en la personne de l'unique juriste du contrôlé qui exerçait d'ailleurs encore d'autres missions. La formation restreinte estime qu'une telle organisation requiert que l'organisme détermine et documente le temps nécessaire au point de contact local pour exercer ses missions relatives à la protection des données afin de pouvoir lui attribuer les ressources nécessaires. Cette exigence résulte notamment des lignes directrices concernant les DPD ainsi que des articles 5.2. et 24 du RGPD qui énoncent le principe de responsabilité (« *accountability* »). Or, il ressort du dossier que le contrôlé n'a pas procédé à une quelconque formalisation ou documentation permettant de démontrer que le contrôlé a fourni à la fonction de DPD les ressources nécessaires à l'exercice de ses missions au moment de l'enquête.

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

c) Sur le manquement 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 États 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 atteint par le contrôlé dans le cadre de cette campagne d'audit, il 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 4, il ressort de l'enquête qu'il n'y a pas de remontée directe d'information du DPD Groupe vers la direction locale du contrôlé. Le chef d'enquête prend note qu'*« il y a plusieurs niveaux de reporting ([…])* », mais estime que « *ces éléments ne sont pas suffisants pour compenser l'absence de reporting direct du DPD vers le responsable de traitement à Luxembourg* ».

42. Dans sa prise de position du 22 novembre 2019, le contrôlé renvoie à ces explications relatives au premier grief, à savoir le manquement à l'obligation d'associer le DPD à toutes les questions relatives à la protection des données à caractère personnel. Par ailleurs, le contrôlé soutient que le DPD Groupe « *informe et conseille le responsable du traitement ainsi que les employés et a notamment mis en œuvre :*

- *Une Formation en ligne […], disponible en ligne à compter de mai 2018*
- *Une Campagne de sensibilisation avec […] sur la protection des données à caractère personnel le […] 2018, ainsi que le […] 2019[…]*
- *Une Campagne de sensibilisation avec […] comprenant les 10 règles d'or sur la protection des données à caractère personnel en date du […] 2019* »

Le contrôlé affirme encore que le DPD Groupe « *a l'occasion d'échanger sur des sujets stratégiques et/ou plus opérationnels avec l'encadrement supérieur […] de la Société A* ».

43. La formation restreinte prend note que le manquement relevé par le chef d'enquête ne concerne que la mission d'information et de conseil du DPD à l'égard du responsable de traitement, et non pas la mission d'information et de conseil du DPD à l'égard des employés.

44. La formation restreinte estime que la mission d'information et de conseil du DPD à l'égard du responsable du traitement est intimement liée à l'obligation, prévue à l'article 38.1 du RGPD, d'associer le DPD de manière appropriée et en temps utile à toutes les questions relatives à la protection des données à caractère personnel. Or, la formation restreinte a constaté que le DPD Groupe n'était pas associé de manière appropriée et en temps utile aux questions de protection des données se posant au niveau de l'entité luxembourgeoise ayant

fait l'objet de l'enquête[9]. En effet, le DPD Groupe n'était associé qu'indirectement, cela par l'intermédiaire du point de contact local. De plus, il était simplement informé des mesures que le [Comité GDPR] propose aux différents organes décisionnels du contrôlé de mettre en œuvre.

45. 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.

III. Sur les mesures correctrices et amendes

A. Les principes

46. 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 CNPD 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;

[9] Points 26 à 30 de la présente décision

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.* »

47. Conformément à l'article 48 de la loi du 1er août 2018, la CNPD peut imposer des amendes administratives telles que prévues à l'article 83 du RGPD, sauf à l'encontre de l'État ou des communes.

48. 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 ».

49. 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.

50. Néanmoins, les démarches effectuées par le contrôlé pour se mettre en conformité avec le RGPD en 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

51. Dans le courrier complémentaire à la communication des griefs du 24 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 18.000 euros.

52. Dans sa note de plaidoiries, le mandataire du contrôlé fait valoir qu'une amende administrative « *doit répondre aux principes d'adéquation et de proportionnalité de l'article 83 du RGPD alors que notamment, aucun grief précis n'a été formulé, aucun préjudice n'a été constaté et la Société A a collaboré dans la mesure du possible avec la CNPD pendant l'ensemble de la période de contrôle*. »

53. 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, 38.2 et 39.1 a) 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, bénéficie des ressources et du temps nécessaires pour exercer ses missions relatives à la protection des données et exerce de façon effective ses missions dont la mission d'information et de conseil du responsable du traitement. Un manquement aux articles 38.1, 38.2 et 39.1 a) du RGPD revient à réduire l'intérêt, voire à vider de sa substance, l'obligation pour un organisme de nommer un DPD.

- Quant au critère de durée (article 83.2.a) du RGPD), la formation restreinte relève que le contrôlé a indiqué, dans sa prise de position du 30 septembre 2020, que le point de contact local a été désigné comme DPD avec effet au 1er octobre 2020 et que ce dernier consacre désormais 50% de son temps de travail aux questions de protection des données, avec l'assistance de […] autres juristes qui y consacrent également chacun 50% de leur temps de travail. En outre, la composition et le fonctionnement du

[Comité GDPR] ont été modifiés de façon à ce que le DPD puisse informer et conseiller le responsable du traitement. Les manquements aux articles 38.1, 38.2 et 39.1 a) ont donc duré dans le temps, à tout le moins entre le 25 mai 2018 et le 1er octobre 2020. La formation restreinte rappelle ici que deux ans ont séparé l'entrée en vigueur du RGPD de son entrée en application pour permettre aux responsables du traitement de se conformer aux obligations qui leur incombent.

- Quant au nombre de personnes concernées affectées par la violation et le niveau de dommage qu'elles ont subi (article 83.2 a) du RGPD), la formation restreinte relève que le contrôlé compte environ […] employés répartis sur […] sites ainsi que […]. Le nombre de personnes concernées par la violation est donc potentiellement élevé.

- 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.

54. 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.

55. La formation restreinte relève que si plusieurs mesures ont été mises en place par le contrôlé afin de remédier en totalité ou en partie à certains manquements, celles-ci n'ont été adoptées 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 49 de la présente décision).

56. 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, 38.2 et 39.1 a) du RGPD.

57. 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, 38.2 et 39.1 a) 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.

58. 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 18.000 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

59. Dans son courrier complémentaire à la communication des griefs, 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 formelle et effective du DPD à toutes les questions relatives à la protection des données, conformément aux exigences de l'article 38 paragraphe 1 du RGPD. Bien que plusieurs manières puissent être envisagées pour parvenir à ce résultat, une des possibilités consisterait à analyser, avec le DPD, tous les comités/groupes de travail pertinents au regard de la protection des données et de formaliser les modalités de son intervention (information antérieure de l'agenda des réunions, invitation, fréquence, statut de membre permanent etc.)*.
>
> *b) Ordonner la mise à disposition des ressources nécessaires au DPD conformément aux exigences de l'article 38 paragraphe 2 du RGPD. Bien que plusieurs manières puissent être envisagées pour parvenir à ce résultat, une des possibilités consisterait à décharger le DPD et/ou les membres locales de son équipe de tout ou partie de ses autres missions/fonctions ou de lui fournir un support formel, en interne ou en externe, quant à l'exercice de ses missions de DPD.*
>
> *c) Ordonner la mise en place de mesures permettant au DPD d'informer et de conseiller formellement le responsable de traitement sur ses 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.* »

60. Quant aux mesures correctrices proposées par le chef d'enquête et par référence au point 50 de la présente décision, la formation restreinte prend en compte les démarches

effectuées par le contrôlé, suite à la visite des agents de la CNPD, afin de se conformer aux dispositions des articles 38.1, 38.2 et 39.1 a) du RGPD, comme détaillées dans ces courriers des 21 novembre 2019 et 30 septembre 2020. Plus particulièrement, elle prend note des faits suivants :

- Quant à la violation de l'article 38.1 du RGPD prévoyant l'obligation d'associer le DPD à toutes les questions relatives à la protection des données à caractère personnel, la formation restreinte prend note que le point de contact local a été désigné DPD de l'organisme contrôlé avec effet au 1er octobre 2020.

  Cependant, la formation restreinte comprend des documents fournis par le contrôlé que ce DPD nouvellement désigné exerce ses fonctions sous la supervision du DPD [du groupe]. La formation restreinte se demande donc si le DPD nouvellement désigné est effectivement associé à toutes les questions relatives à la protection des données à caractère personnel, et ceci en toute indépendance. Par conséquent, la CNPD est d'avis que le contrôlé n'a pas démontré avec suffisance sa mise en conformité avec l'article 38.1 du RGPD et considère qu'il y a lieu de prononcer une mesure de mise en conformité à cet égard.

- En ce qui concerne la violation de l'article 38.2 du RGPD prévoyant l'obligation de fournir les ressources nécessaires au DPD, le contrôlé affirme dans sa prise de position du 30 septembre 2020 que le DPD nouvellement désigné par la Société A consacre 50% de son temps de travail aux questions de protection des données et qu'il est assisté de […] juristes qui y consacrent […] de sorte qu'il y aura 1,5 ETP consacrés à la protection des données à caractère personnel.
  Au regard de ces éléments, la formation restreinte est d'avis que l'attente du chef d'enquête de 1 ETP ou plus est atteinte suite aux mesures prises par le contrôlé au cours de l'enquête. Par conséquent, la formation restreinte considère qu'il n'y a pas lieu de prononcer une mesure de mise en conformité à cet égard.

- Quant à la violation de l'article 39.1 a) du RGPD relatif à la mission d'information et de conseil du DPD envers le responsable du traitement, le contrôlé expose dans sa prise de position du 30 septembre 2020 la composition et le fonctionnement du [Comité GDPR] qui permettra au DPD nouvellement désigné d'informer et de conseiller le responsable du traitement.

Cependant, au regard des documents fournis par le contrôlé, la formation restreinte comprend que le DPD (auparavant point de contact local, sans avoir exercé la fonction de DPD) nouvellement désigné par le contrôlé exerce ses missions sous la supervision du DPD [du groupe], de telle sorte qu'il n'est pas démontré avec suffisance par le contrôlé que le DPD nouvellement désigné puisse effectivement remplir sa mission d'information et de conseil envers le responsable du traitement contrôlé (Société A), et ceci en toute indépendance. Par conséquent, la formation restreinte estime qu'il y a lieu de prononcer une mesure de mise en conformité à cet égard.

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

- de prononcer à l'encontre de la société « Société A » une amende administrative d'un montant de dix-huit mille euros (18.000 euros) au regard de la violation des articles 38.1, 38.2 et 39.1. a) du RGPD ;

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

s'assurer que le DPD soit effectivement associé à toutes les questions relatives à la protection des données à caractère personnel, et ceci en toute indépendance ;

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

s'assurer que le DPD puisse effectivement remplir sa mission d'information et de conseil envers le responsable du traitement contrôlé.

Ainsi décidé à Belvaux en date du 31 mai 2021.

Pour 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.