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

Délibération n° 10FR/2021 du 26 mars 2021

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

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE;

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

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

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

Considérant ce qui suit :

I. Faits et procédure

1. Vu l'impact du rôle du délégué à la protection des données (ci-après : le « DPD ») et l'importance de son intégration dans l'organisme, et considérant que les lignes directrices concernant les DPD sont disponibles depuis décembre 2016[1], soit 17 mois avant l'entrée en application du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

[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.

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-[…] et inscrite au registre de commerce et des sociétés sous le numéro […] (ci-après : « Société A » ou le « contrôlé ») et de désigner M. Christophe Buschmann comme chef d'enquête. Ladite délibération précise que l'enquête porte sur la conformité de la Société A avec la section 4 du chapitre 4 du RGPD.

3. La Société A a pour objet de faire toutes opérations d'assurances, de coassurances et de réassurances, […]. A la fin de l'exercice 2018, elle occupait […] personnes[2] et elle compte environ […] clients par an[3].

4. Par courrier du 17 septembre 2018, le chef d'enquête a envoyé un questionnaire préliminaire à la Société A auquel cette dernière a répondu par courrier du 3 octobre 2018. Une visite sur place a eu lieu le 30 janvier 2019. Suite à ces échanges, le chef d'enquête a établi le rapport d'audit n°[…] (ci-après : le « rapport d'audit »).

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

1) S'assurer que l'organisme soumis à l'obligation de désigner un DPD l'a bien fait ;
2) S'assurer que l'organisme a publié les coordonnées de son DPD ;
3) S'assurer que l'organisme a communiqué les coordonnées de son DPD à la CNPD ;
4) S'assurer que le DPD dispose d'une expertise et de compétences suffisantes pour s'acquitter efficacement de ses missions ;

[2] Rapport annuel 2018 de la Société A.
[3] Réponse fournie par la Société A dans le questionnaire préliminaire du 17 septembre 2018.

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 5 février 2020 (ci-après : la « communication des griefs »), le chef d'enquête a informé la Société A des manquements aux obligations prévues par le RGPD qu'il a relevés lors de son enquête. Le rapport d'audit était joint audit courrier.

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

- l'obligation de désigner le DPD sur base de ses qualités professionnelles[4] ;
- l'obligation de communiquer les coordonnées du DPD à l'autorité de contrôle[5] ;
- l'obligation d'associer le DPD à toutes les questions relatives à la protection des données à caractère personnel[6] ;
- l'obligation de garantir l'autonomie du DPD[7] ;
- la mission de contrôle du DPD[8].

8. Par courrier du 25 février 2020, la Société A a adressé au chef d'enquête sa prise de position quant aux manquements énumérés dans la communication des griefs. En ce qui concerne le manquement relatif à la garantie de l'autonomie du DPD, le contrôlé affirme dans ledit courrier que « *le DPD fait partie de l'équipe […] rattachée directement au Directeur*

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

Général, la personne dont [le DPD] dépend est le Chief Compliance Officer […]. Le DPD fait bien rapport directement au Directeur Général, un meeting récurrent hebdomadaire est d'ailleurs fixé et en cas d'urgence, une entrevue est fixée dans la journée. » Concernant le manquement relatif à la mission de contrôle, la Société A fait valoir, dans son courrier du 25 février 2020, qu'« *[u]n plan de contrôle avait été établi pour 2019 (voir annexe 2), il a été présenté le 15/01/2019 et validé par le […]) […] ».* Le contrôlé a par ailleurs transmis des pièces supplémentaires par email du 26 août 2020, à savoir deux exemples relatifs au fonctionnement et aux passages par le […] et le […].

9. Le 4 septembre 2020, le chef d'enquête a adressé à la Société A un courrier complémentaire à la communication des griefs par lequel il informe le contrôlé que suite à sa prise de position du 25 février 2020 et des pièces fournies par email en date du 26 août 2020, il y a lieu de lever les griefs relatifs à l'autonomie et aux missions de contrôle du DPD. Etait jointe au courrier du 4 septembre 2020 une communication des griefs modificative (ci-après : la « communication des griefs modificative ») intégrant les mesures correctrices que le chef d'enquête propose à la Commission nationale siégeant en formation restreinte (ci-après : la « formation restreinte ») d'adopter.

10. Par courrier du 15 septembre 2020, la Société A a fait parvenir au chef d'enquête ses observations quant à la communication des griefs modificative.

11. Lors de l'examen du dossier d'enquête, la formation restreinte n'a par ailleurs pas constaté d'autres éléments qui seraient constitutifs d'un manquement relatif à l'autonomie ou à la mission de contrôle du DPD.

12. L'affaire a été à l'ordre du jour de la séance de la formation restreinte du 13 novembre 2020. Conformément à l'article 10, point 2, lettre b) du règlement d'ordre intérieur de la Commission nationale, le chef d'enquête et le contrôlé ont présenté des observations orales sur l'affaire et ont répondu aux questions posées par la formation restreinte. La Société A a eu la parole en dernier.

II. En droit

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

1. Sur les principes

13. Selon l'article 37(5) du RGPD, « *[le DPD] est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données […]* ».

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

15. Par ailleurs, le groupe de travail « Article 29 » sur la protection des données a adopté le 13 décembre 2016 des lignes directrices concernant les DPD qui ont été reprises et réapprouvées par le comité européen de la protection des données en date du 25 mai 2018[9]. Ces lignes directrices précisent que le niveau d'expertise du DPD « *doit être proportionné à la sensibilité, à la complexité et au volume des données traitées par un organisme* »[10] et qu'« *il est nécessaire que les DPD disposent d'une expertise dans le domaine des législations et pratiques nationales et européennes en matière de protection des données, ainsi que d'une connaissance approfondie du RGPD* »[11].

16. Les lignes directrices concernant les DPD poursuivent que « *[l]a connaissance du secteur d'activité et de l'organisme du responsable du traitement est utile. Le DPD devrait également disposer d'une bonne compréhension des opérations de traitement effectuées, ainsi que des systèmes d'information et des besoins du responsable du traitement en matière de protection et de sécurité des données* »[12].

2. En l'espèce

17. Il résulte du rapport d'audit que dans le cadre de cette campagne d'audit, le chef d'enquête attend que le DPD ait au minimum trois ans d'expérience professionnelle en matière de protection des données.

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

18. Selon le point 20 de la communication des griefs modificative, il a été constaté lors de l'enquête que le DPD dispose de moins de trois ans d'expérience en matière de protection des données et qu'antérieurement à sa prise de fonction en […] 2018, il occupait la fonction de *[…]*. Le point 21 de la communication des griefs modificative énumère les évènements et formations en lien avec la protection des données auxquels le DPD a assisté après sa prise de fonction.

19. Néanmoins, le chef d'enquête estime que ces formations ne suffisent pas à établir l'existence d'une expertise suffisante et adaptée aux besoins du responsable du traitement en matière de protection des données au moment de l'enquête de sorte qu'il y a un manquement à l'obligation prévue à l'article 37(5) du RGPD.

20. Dans ses prises de position des 25 février et 15 septembre 2020, la Société A fait valoir que le DPD continue à suivre des formations et à participer à des évènements et groupes de travail en lien avec la protection des données de sorte que le DPD aura atteint trois années d'expérience en […] 2021.

21. Il ressort ainsi de la communication des griefs modificative et des prises de position du contrôlé qu'antérieurement à sa prise de fonction en […] 2018, le DPD n'avait aucune expérience professionnelle en matière de protection des données.

22. La formation restreinte prend note qu'en 2018 et 2019, le DPD a assisté à un certain nombre de formations et d'évènements relatifs à la protection des données. Elle se rallie toutefois au constat du chef d'enquête selon lequel ces formations ne sauraient suffire à établir, au moment de l'enquête, l'existence d'une expertise suffisante et adaptée aux besoins du contrôlé en matière de protection des données.

23. Au vu de ce qui précède, la formation restreinte conclut que l'article 37(5) du RGPD n'a pas été respecté par la Société A.

B. <u>Sur le manquement à l'obligation de communiquer les coordonnées du DPD à l'autorité de contrôle</u>

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

24. L'article 37(7) du RGPD prévoit l'obligation pour l'organisme de communiquer les coordonnées du DPD à l'autorité de contrôle. En effet, il résulte de l'article 39(1) e) du RGPD que le DPD fait office de point de contact pour l'autorité de contrôle de sorte qu'il est important que cette dernière dispose des coordonnées du DPD.

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

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

2. <u>En l'espèce</u>

27. Il résulte du rapport d'audit que le chef d'enquête attend que l'organisme doit avoir communiqué au 25 mai 2018 les coordonnées de son DPD à la CNPD.

28. Selon le point 24 de la communication des griefs modificative, la Société A a communiqué à la CNPD les coordonnées du DPD qui était en fonction au moment de l'enquête par email du […] 2018. Le DPD précédemment en place n'a pas fait l'objet d'une déclaration en application du RGPD.

29. Dans sa prise de position du 25 février 2020, le contrôlé soutient que les coordonnées du premier DPD ont été communiquées le […] 2017 et que lors de son départ […], il a été remplacé par le DPD actuellement en fonction.

30. La formation restreinte constate que le RGPD est applicable depuis le 25 mai 2018 de sorte que l'obligation de communiquer les coordonnées du DPD à l'autorité de contrôle existe depuis cette date.

31. Même si le chargé à la protection des données tel que prévu par la loi abrogée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel peut être qualifié de précurseur du DPD dans la mesure où il y a des similarités entre les deux fonctions, il n'en demeure pas moins qu'il existe des différences,

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

notamment au niveau de la désignation et de la législation ancienne et nouvelle. Ainsi, les chargés de la protection des données désignés sous la loi abrogée du 2 août 2002 ne prenaient pas automatiquement la fonction de DPD et les organismes qui avaient désigné volontairement un tel chargé sous l'ancienne loi devaient tout de même se conformer aux articles 37 à 39 du RGPD, et notamment communiquer les coordonnées du DPD à la CNPD.

32. En tout état de cause, il ressort du rapport d'audit que l'ancien chargé de la protection des données n'a pas été désigné comme DPD mais qu'un […] interne assurait cette fonction entre le 25 mai 2018, date d'entrée en application du RGPD, et le […] 2018, date de prise de fonction du DPD actuellement en fonction. Or, les coordonnées du DPD qui était en fonction entre le 25 mai 2018 et le […] 2018 n'ont pas été communiquées à la CNPD. Les coordonnées du DPD actuellement en fonction ont été communiquées le […] 2018.

33. Au vu de ce qui précède, la formation restreinte conclut que l'article 37(7) du RGPD n'a pas été respecté par la Société A.

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

1. Sur les principes

34. 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.

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

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

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

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

37. 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. <u>En l'espèce</u>

38. Il ressort du rapport d'audit que dans le cadre de cette campagne d'audit, le chef d'enquête attend 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.

39. Selon les points 28 et 29 de la communication des griefs modificative, le DPD participe principalement sur invitation ad hoc aux différents comités du contrôlé, comme par exemple le […], le […] ou le […], sans qu'une participation régulière et systématique ne soit prévue. Le DPD est informé par le responsable […] des discussions ayant lieu au […]. Les comptes rendus […] sont envoyés au DPD qui ne participe pas à ces réunions.

40. Dans ses prises de position des 25 février et 15 septembre 2020, la Société A fait valoir que le DPD participe personnellement de manière systématique au […] et qu'il participe également au […] de manière ad hoc pour les sujets relatifs à la protection des données. Pour tous les projets ou changements significatifs dans un processus, le Project Manager doit systématiquement compléter un questionnaire […] qui est soumis au DPD […] pour évaluation des impacts sur la protection des données et déclenchement d'une analyse d'impact si

nécessaire. Le contrôlé soutient encore que le DPD est informé de tout nouveau projet grâce à sa participation au […].

41. La formation restreinte note qu'au point 30 de la communication des griefs modificative, le chef d'enquête parvient à la conclusion que « *[s]'il n'est pas contesté que le fonctionnement du responsable du traitement permet au DPD d'être raisonnablement informé sur les questions de protection de données à caractère personnel*, *l'absence de mécanisme permettant l'implication personnelle régulière et systématique du DPD n'est pas de nature à garantir un* niveau d'association suffisant et adapté aux besoins du responsable de traitement. »

42. Même s'il est vrai que l'article 38(1) du RGPD n'exige pas que l'organisme mette en place des mesures spécifiques pour assurer l'association du DPD à toutes les questions relatives à la protection des données à caractère personnel, il est vrai aussi que les lignes directrices concernant les DPD, qui formulent des recommandations et des bonnes pratiques, guident les responsables de traitement dans la mise en conformité à l'égard de leur gouvernance. Or, la formation restreinte n'a pas identifié d'éléments dans le dossier d'enquête permettant de conclure que le DPD n'était pas associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

43. Au vu de ce qui précède, la formation restreinte conclut que le manquement à l'article 38(1) du RGPD n'est pas constitué.

III. Sur les mesures correctrices et l'amende

44. 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 du RGPD.

45. Aux termes de l'article 58(2) du RGPD, « *[c]haque autorité de contrôle dispose du pouvoir d'adopter toutes les mesures correctrices suivantes:*

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.* »

46. Dans la communication des griefs modificative, le chef d'enquête propose à la formation restreinte de prendre la mesure correctrice suivante : « *Mettre en place les mesures permettant au DPD (ou une équipe « Data Protection » dédiée) d'acquérir une expertise suffisante et adaptée aux besoins du responsable de traitement en matière de protection des*

données, conformément aux dispositions de l'article 37, paragraphe (5) du RGPD et aux lignes directrices relatives au DPD du groupe de travail « article 29 » sur la protection des données qui précisent que le niveau d'expertise du DPD doit être proportionné à la sensibilité, à la complexité et au volume des données traitées par l'organisme. La poursuite de l'effort de formation du DPD est une possibilité pour parvenir à ce résultat. »

47. Le chef d'enquête propose également de *«[m]ettre en place les mesures permettant d'associer le DPD à toutes les questions relatives à la protection des données, conformément aux exigences de l'article 38 paragraphe 1 du RGPD. Bien que plusieurs manières puissent être envisagées pour parvenir à ce résultat, une des possibilités pourrait être de renforcer l'implication personnelle et systématique du DPD aux différents comités pertinents.* » Etant donné que la formation restreinte estime que le manquement allégué par le chef d'enquête relatif à l'obligation d'associer le DPD à toutes les questions relatives à la protection des données n'est pas constitué, il n'y a pas lieu d'examiner la mesure correctrice y afférente.

48. Finalement, compte tenu des faits constatés au début de l'enquête et des circonstances particulières de l'espèce, le chef d'enquête suggère à la formation restreinte de ne pas retenir une amende administrative en plus des mesures correctrices.

A. Le rappel à l'ordre

49. En vertu de l'article 58(2) b) du RGPD, la CNPD peut rappeler à l'ordre un responsable du traitement ou un sous-traitant lorsque les opérations de traitement ont entraîné une violation des dispositions du RGPD.

50. Compte tenu du fait que le contrôlé a violé l'article 37(5) et (7) du RGPD, la formation restreinte considère qu'il est justifié de prononcer un rappel à l'ordre à l'encontre de la Société A.

B. La mise en conformité des opérations de traitement

51. En vertu de l'article 58(2) d) du RGPD, la CNPD peut ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec le RGPD, le cas échéant, de manière spécifique et dans un délai déterminé.

52. Quant à la violation de l'article 37(5) du RGPD prévoyant l'obligation de désigner le DPD sur la base de ses qualités professionnelles, il ressort du point 34 de la communication des griefs modificative que le contrôlé a « *proactivement mis en place un programme de*

formation à destination du DPD tant sur la protection des données personnelles, sur la cybersécurité ou la sécurité des systèmes d'information que sur la […] et du fonctionnement du responsable du traitement ». Par conséquent, la formation restreinte considère qu'il n'y a pas lieu de prononcer une mesure de mise en conformité à cet égard, d'autant plus que le DPD pourra bientôt faire preuve de trois ans d'expérience professionnelle en matière de protection des données.

53. Quant à la violation de l'article 37(7) du RGPD prévoyant l'obligation de communiquer les coordonnées du DPD à l'autorité de contrôle, la formation restreinte constate que la Société A a communiqué à la CNPD les coordonnées du DPD actuellement en fonction par email du […] 2018. Par conséquent, la formation restreinte considère qu'il n'y a pas lieu de prononcer une mesure de mise en conformité à cet égard.

C. L'amende administrative

54. En vertu de l'article 58(2) i) du RGPD, la CNPD peut imposer une amende administrative en application de l'article 83, en complément ou à la place des mesures visées à ce paragraphe, en fonction des caractéristiques propres à chaque cas. L'article 48(1) de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données précise que la CNPD peut imposer les amendes administratives telles que prévues à l'article 83 du RGPD, sauf à l'encontre de l'État ou des communes.

55. Selon l'article 83(2) du RGPD, « *[p]our décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative, il est dûment tenu compte, dans chaque cas d'espèce, des éléments suivants:*

> *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. »

56. Il résulte du point 34 de la communication des griefs modificative que le chef d'enquête a pris en compte « *les faits au moment de l'ouverture de l'enquête et les éléments suivants :*

- *Le fait que le DPD soit une pierre angulaire du principe de responsabilisation et qu'il soit au cœur du cadre juridique instauré par le RGPD ;*
- *Le fait qu'il n'est pas contesté que le fonctionnement du responsable de traitement permette au DPD d'être raisonnablement informé ;*
- *Le fait que le responsable de traitement ait proactivement mis en place un programme de formation à destination du DPD tant sur la protection des données personnelles, sur la cybersécurité ou la sécurité des systèmes d'information que sur la […] et du fonctionnement du responsable de traitement »*.

57. Ainsi, le chef d'enquête suggère à la formation restreinte de ne pas retenir une amende administrative en plus des mesures correctrices.

58. La formation restreinte se rallie aux développements du chef d'enquête et estime par conséquent qu'il n'y a pas lieu d'imposer une amende administrative à l'encontre de la Société A.

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 A, établie et ayant son siège social à L-[…] et inscrite au registre de commerce et des sociétés sous le numéro […], un rappel à l'ordre pour avoir violé l'article 37 (5) et (7) du RGPD.

Ainsi décidé à Belvaux en date du 26 mars 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.