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

Délibération n° 19FR/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-[…] et inscrite au registre de commerce et des sociétés sous le numéro […] (ci-après : « Société A » ou le « contrôlé ») et de désigner Monsieur 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. Le contrôlé a pour objet de faire toutes opérations d'assurance, de coassurances et de réassurances […] au Grand-Duché de Luxembourg. Au début de l'année 2019, la Société A occupait environ […] employés au siège de la compagnie (sans prendre en compte les personnes dans les différentes agences) et comptait environ […] clients […][2].

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 8 octobre 2018. Une visite sur place a eu lieu le 18 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] Compte-rendu de la Visite du 18 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 23 octobre 2019 (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 un manquement à l'obligation de veiller à ce que les missions et tâches du DPD n'entraînent pas de conflit d'intérêts[3].

[3] Objectif n° 5

8. Par courrier du 21 novembre 2019, la Société A a adressé au chef d'enquête sa prise de position quant au manquement énuméré dans la communication des griefs. Le contrôlé affirme dans ledit courrier que « *différentes mesures sont déjà mises en œuvre au sein de la Société A et plus généralement du groupe […] pour éviter un tel conflit d'intérêts* » et que les rôles de Chief Compliance Officer et DPD sont occupés par des personnes différentes depuis […] 2019.

9. Le 10 août 2020, le chef d'enquête a adressé à la Société A un courrier complémentaire à la communication des griefs (ci-après : le « courrier complémentaire à la communication des griefs ») par lequel il informe le contrôlé de la mesure correctrice 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 17 septembre 2020, le contrôlé a fait parvenir au chef d'enquête ses observations quant à la communication des griefs complémentaire.

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 présenté des observations orales sur l'affaire et ont répondu aux questions posées par la formation restreinte. Le contrôlé a eu la parole en dernier.

II. En droit

1. Sur les principes

12. Selon l'article 38.6 du RGPD, « *[le DPD] peut exécuter d'autres missions et tâches. Le responsable du traitement ou le sous-traitant veille à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts* ».

13. Les lignes directrices concernant les DPD[4] précisent que le DPD ne peut exercer au sein de l'organisme une fonction qui l'amène à déterminer les finalités et les moyens du traitement de données à caractère personnel. D'une manière générale, parmi les fonctions susceptibles de donner lieu à un conflit d'intérêts au sein de l'organisme peuvent figurer les fonctions

[4] WP 243 v.01, version révisée et adoptée le 5 avril 2017, pp.19-20

d'encadrement supérieur (par exemple : directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du service informatique), mais aussi d'autres rôles à un niveau inférieur de la structure organisationnelle si ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement. En outre, il peut également y avoir conflit d'intérêts, par exemple, si un DPD externe est appelé à représenter le responsable du traitement ou le sous-traitant devant les tribunaux dans des affaires ayant trait à des questions liées à la protection des données.

En fonction des activités, de la taille et de la structure de l'organisme, il peut être de bonne pratique pour les responsables du traitement ou les sous-traitants :

- de recenser les fonctions qui seraient incompatibles avec celle de DPD ;
- d'établir des règles internes à cet effet, afin d'éviter les conflits d'intérêts ;
- d'inclure une explication plus générale concernant les conflits d'intérêts ;
- de déclarer que le DPD n'a pas de conflit d'intérêts en ce qui concerne sa fonction de DPD, dans le but de mieux faire connaître cette exigence ;
- de prévoir des garanties dans le règlement intérieur de l'organisme, et de veiller à ce que l'avis de vacance pour la fonction de DPD ou le contrat de service soit suffisamment précis et détaillé pour éviter tout conflit d'intérêts. Dans ce contexte, il convient également de garder à l'esprit que les conflits d'intérêts peuvent prendre différentes formes selon que le DPD est recruté en interne ou en externe.

2. <u>En l'espèce</u>

14. Il résulte du rapport d'audit que, pour que le chef d'enquête considère l'objectif 5 comme atteint par le contrôlé dans le cadre de cette campagne d'audit, le chef d'enquête s'attend à ce que, dans le cas où le DPD exerce d'autres fonctions au sein de l'organisme contrôlé, ces fonctions n'entraînent pas de conflit d'intérêts notamment par l'exercice de fonctions qui amènerait le DPD à déterminer les finalités et les moyens du traitement de données à caractère personnel. Le chef d'enquête s'attend également à ce que le contrôlé ait réalisé une analyse quant à l'existence d'un éventuel conflit d'intérêts au niveau du DPD.

15. Selon la communication des griefs, il ressort de l'enquête que le DPD est également Chief Compliance Officer de l'organisme contrôlé et que cette autre fonction implique un risque de conflit d'intérêts, notamment dans le cadre des traitements AML/KYC du département Compliance. Par conséquent, le DPD serait impliqué dans la mise en place de traitements de données à caractère personnel dans le cadre de ses fonctions de Chief Compliance Officer.

16. Dans ses prises de position des 21 novembre 2019 et 17 septembre 2020, la Société A fait valoir l'existence, en janvier 2019, de différentes mesures ayant pour objectif d'éviter un tel conflit d'intérêts.

17. La Société A explique d'une part que son organisation structurelle est constituée de trois lignes de défense :

- Une première ligne de défense, […] ;
- Une deuxième ligne de défense […] ;
- Une troisième ligne de défense […].

18. Selon la Société A, ce concept des trois lignes de défense « *permet de prévenir au mieux les conflits d'intérêts dans tout domaine confondu en organisant une ségrégation des différentes fonctions. Ainsi, la fonction de DPD au sein de la Société A, […], exclut de traiter les données relatives aux traitements AML/KYC et les finalités et moyens du traitement sont décidées uniquement par les équipes […]. Le DPD au sein de la Société A pourrait être amené à se prononcer sur la conformité des traitements mis en en œuvre par les équipes […], […]* ».

19. La Société A ajoute également dans sa prise de position du 21 novembre 2019 que « *le Chief Compliance Officer ne fait que contrôler que les décisions prises […] sont conformes aux exigences du groupe […] et aux lois et normes applicables et n'intervient qu'à titre de conseil ; il s'assure de l'efficience et de l'efficacité des contrôles sur les activités opérationnelles AML/KYC en tant que telles, […]* ».

20. D'autre part, la Société A est dotée d'une politique de gestion des conflits internes et externes, prévoyant qu'en cas d'un éventuel conflit d'intérêts qui impacterait la fonction de DPD, ce dernier informe le […] et le […] afin de prendre les mesures nécessaires.

21. En outre, il ressort des prises de position par la Société A des 21 novembre 2019 et 17 septembre 2020 que le contrôlé a nommé en […] 2019 un nouveau DPD de façon à ce que les fonctions de DPD et de Chief Compliance Officer ne soient plus cumulées dans le chef d'une unique personne. Le nouveau DPD exerce également les fonctions de […] de la Société A.

22. La formation restreinte prend note de l'existence de ces mesures afin de limiter les risques de conflit d'intérêts au sein de l'organisme contrôlé. Elle se rallie toutefois au constat du chef d'enquête selon lequel la mise en œuvre de ces différentes mesures ne saurait suffire à établir, au moment de l'enquête, l'absence de risque de conflit d'intérêts dans le cadre des missions du DPD. En effet, il n'est pas établi avec suffisance que le Chief Compliance Officer, cumulant cette fonction avec celle de DPD au moment de l'enquête, ne participe pas à la détermination des finalités et des moyens du traitement de données à caractère personnel mis en œuvre dans le cadre des activités opérationnelles AML/KYC.

23. Au vu de ce qui précède, la formation restreinte conclut que l'article 38(6) du RGPD n'a pas été respecté par la Société A.

III. Sur les mesures correctrices et l'amende

A. Les principes

24. 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 ;*

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 adressées à un destinataire situé dans un pays tiers ou à une organisation internationale.* »

25. 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.

26. 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 35 ;

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*. »

27. 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.

28. 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. <u>En l'espèce</u>

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

29. Il résulte de la communication des griefs et de la communication des griefs complémentaire que le chef d'enquête ne propose pas d'amende administrative à l'encontre du contrôlé.

30. 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.

2. <u>Quant au rappel à l'ordre</u>

31. 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.

32. Compte tenu du fait que le contrôlé a violé l'article 38(6) du RGPD, la formation restreinte considère qu'il est justifié de prononcer un rappel à l'ordre à l'encontre de la Société A .

3. Quant à la prise de mesures correctrices

33. Dans la communication des griefs complémentaire, le chef d'enquête propose à la formation restreinte de prendre la mesure correctrice suivante : « *ordonner la mise en place de mesures assurant que les différentes missions et tâches, actuelles ou passées, de la personne exerçant la fonction DPD n'entraînent pas de conflit d'intérêts conformément aux exigences de l'article 38 paragraphe 6 du RGPD. Bien que plusieurs manières puissent être mises en œuvre pour parvenir à ce résultat, une des possibilités serait d'impliquer une tierce personne, bénéficiant des compétences nécessaires, pour la revue des traitements pour lesquels il existe un conflit d'intérêts (en l'occurrence les traitements AML/KYC). Une autre possibilité serait d'occuper le poste de DPD par une personne différente du Compliance Officer et ne disposant pas d'un autre risque de conflit* ».

34. Par référence au point 21 de la présente décision, la formation restreinte prend en compte les démarches effectuées par le contrôlé suite à la communication des griefs envoyée au contrôlé par le chef d'enquête, afin de se conformer aux dispositions de l'article 38.6 du RGPD, comme détaillées dans ces courriers des 21 novembre 2019 et 17 septembre 2020. Plus particulièrement, la formation restreinte prend note du fait que le contrôlé a nommé, en […] 2019, un nouveau DPD de façon à ce que les fonctions de DPD et de Chief Compliance Officer ne soient plus cumulées dans le chef d'une unique personne et que le nouveau DPD exerce également les fonctions de […] de la Société A.

35. Cependant, la formation restreinte considère que le contrôlé n'a pas démontré que la nomination d'un nouveau DPD, avec la séparation des fonctions de Chief Compliance Officer,

suffisait en elle-même à supprimer tout risque de conflit d'intérêts dans le cadre de l'exercice des missions de DPD. Par conséquent, la formation restreinte considère que le contrôlé n'a pas démontré avec suffisance sa mise en conformité avec l'article 38.6 du RGPD et 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 A, un rappel à l'ordre au regard de la violation de l'article 38.6 du RGPD ;

- de prononcer à l'encontre de la […] Société A, une injonction de se mettre en conformité avec l'article 38.6 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 :

  éliminer tout risque de conflit d'intérêts dans l'exercice de ses missions par le DPD.

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.