

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

Délibération n° 37FR/2021 du 13 octobre 2021

La Commission nationale pour la protection des données siégeant en formation restreinte, composée de Madame Tine A. Larsen, présidente, et de Messieurs Thierry Lallemand 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 1<sup>er</sup> 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<sup>1</sup>, 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

---

<sup>1</sup> Les lignes directrices concernant les DPD ont été adoptées par le groupe de travail « Article 29 » le 13 décembre 2016. La version révisée (WP 243 rev. 01) a été adoptée le 5 avril 2017.

(règlement général sur la protection des données) (ci-après : le « RGPD »), la Commission nationale pour la protection des données (ci-après : la « Commission nationale » ou la « CNPD ») a décidé de lancer une campagne d'enquête thématique sur la fonction du DPD. Ainsi, 25 procédures d'audit ont été ouvertes en 2018, concernant tant le secteur privé que le secteur public.

2. En particulier, la Commission nationale a décidé par délibération n°[...] du 14 septembre 2018 d'ouvrir une enquête sous la forme d'audit sur la protection des données auprès de la Société A située au [...], L[...] et enregistrée au registre du commerce et des sociétés luxembourgeois sous le n°[...] (ci-après : le « contrôlé ») et de désigner M. Christophe Buschmann comme chef d'enquête. Ladite délibération précise que l'enquête porte sur la conformité du contrôlé avec la section 4 du chapitre 4 du RGPD.

3. Suivant l'article 3 de ses statuts, le contrôlé a pour objet [de faire toutes opérations d'assurance et de réassurance de la branche « Vie » [...].

4. Par courrier du 17 septembre 2018, le chef d'enquête a envoyé un questionnaire préliminaire au contrôlé auquel ce dernier a répondu par courriel du 8 octobre 2018. Une visite sur place a eu lieu le 4 février 2019. Suite à ces échanges, le chef d'enquête a établi le rapport d'audit n°[...] (ci-après : le « rapport d'audit »).

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

- 1) S'assurer que l'organisme soumis à l'obligation de désigner un DPD l'a bien fait ;
- 2) S'assurer que l'organisme a publié les coordonnées de son DPD ;
- 3) S'assurer que l'organisme a communiqué les coordonnées de son DPD à la CNPD ;
- 4) S'assurer que le DPD dispose d'une expertise et de compétences suffisantes pour s'acquitter efficacement de ses missions ;
- 5) S'assurer que les missions et les tâches du DPD n'entraînent pas de conflit d'intérêt ;
- 6) S'assurer que le DPD dispose de ressources suffisantes pour s'acquitter efficacement de ses missions ;
- 7) S'assurer que le DPD est en mesure d'exercer ses missions avec un degré suffisant d'autonomie au sein de son organisme ;

- 8) S'assurer que l'organisme a mis en place des mesures pour que le DPD soit associé à toutes les questions relatives à la protection des données ;
- 9) S'assurer que le DPD remplit sa mission d'information et de conseil auprès du responsable du traitement et des employés ;
- 10) S'assurer que le DPD exerce un contrôle adéquat du traitement des données au sein de son organisme ;
- 11) S'assurer que le DPD assiste le responsable du traitement dans la réalisation des analyses d'impact en cas de nouveaux traitements de données.

6. Par courrier du 24 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 de communiquer les coordonnées du DPD à l'autorité de contrôle<sup>2</sup> ;
- l'obligation de veiller à ce que les missions et tâches du DPD n'entraînent pas de conflit d'intérêts<sup>3</sup>.

8. Par courriel du 27 novembre 2019, le contrôlé a pris position sur le manquement relevé par le chef d'enquête concernant l'obligation de veiller à ce que les missions et tâches du DPD n'entraînent pas de conflits d'intérêts.

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

10. Par courriel du 5 août 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 16 juin 2021. Conformément à l'article 10.2. b) du règlement d'ordre intérieur de la Commission nationale,

---

<sup>2</sup> Objectif n°3

<sup>3</sup> Objectif n°5

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

## II. En droit

### A. Sur le manquement à l'obligation de communiquer les coordonnées du DPD à l'autorité de contrôle

#### 1. Sur les principes

12. 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.

13. 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* »<sup>4</sup>.

14. 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. En l'espèce

15. Il ressort du rapport d'audit que, pour que le chef d'enquête considère l'objectif 3 comme rempli par le contrôlé dans le cadre de cette campagne d'audit, le chef d'enquête s'attend à ce que l'organisme ait communiqué au 25 mai 2018 les coordonnées de son DPD à la CNPD.

16. D'après la communication des griefs, page 2, « [i]l ressort de l'enquête que le formulaire de déclaration du DPD a été envoyé à la CNPD le 28 septembre 2018. La communication a donc été effectuée tardivement. »

17. Le contrôlé n'est pas revenu sur ce manquement dans sa prise de position du 27 novembre 2019, ni lors des échanges ultérieurs avec la CNPD.

---

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

18. 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. Ainsi, la communication des coordonnées du DPD à la CNPD en date du 28 septembre 2018 était tardive.

19. Au vu de ce qui précède, la formation restreinte conclut que l'article 37.7 du RGPD n'a pas été respecté par le contrôlé.

**B. Sur le manquement relatif à l'obligation de veiller à ce que les autres missions et tâches du DPD n'entraînent pas de conflit d'intérêts**

**1. Sur les principes**

20. 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* ».

21. Les lignes directrices concernant les DPD<sup>5</sup> 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* ». Selon les lignes directrices, « *[e]n règle générale, parmi les fonctions susceptibles de donner lieu à un conflit d'intérêts au sein de l'organisme peuvent figurer les fonctions 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 ;*

---

<sup>5</sup> WP 243 v.01, version révisée et adoptée le 5 avril 2017, pp.19-20

- *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 à l'extérieur. »*

## 2. En l'espèce

22. 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, il 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.

23. D'après la communication des griefs, page 3, « [i]l ressort de l'enquête que le DPD est également Head of Compliance, Money Laundering Reporting Officer. Cette autre fonction implique un risque de conflit d'intérêt, notamment dans le cadre des traitements AML du département Compliance. En effet, les lignes directrices relatives au DPD du groupe de travail « article 29 » sur la protection des données indiquent que le DPD ne peut pas 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. [Le contrôlé] a informé la CNPD qu'en cas d'éventuels conflits d'intérêt au niveau des traitements AML du département Compliance, les traitements concernés seraient alors contresignés par le supérieur hiérarchique du DPD. Néanmoins, le DPD reste impliqué dans la mise en place de traitements de données à caractère personnel dans le cadre de ses fonctions de Head of Compliance. Lors de l'enquête, la CNPD n'a pas eu connaissance d'autres éléments permettant d'adresser ce risque, comme par exemple la nomination d'un DPD suppléant (extérieur au département AML) qui serait en charge d'analyser les traitements AML. »

24. Par courriel du 25 novembre 2019, le contrôlé a indiqué que deux délégués suppléants ont été nommés, à savoir le « *Chief Risk Officer (pour les traitements de données personnelles du département Compliance)* » ainsi qu'un « *Senior Compliance Specialist (pour tous les traitements de données personnelles autres que ceux du département Compliance)* ».

25. Le contrôlé a également transmis, avec sa prise de position du 27 novembre 2019, plusieurs documents internes concernant les mesures prises suite au manquement relevé par le chef d'enquête ; ces documents permettent notamment de vérifier les indications fournies par le contrôlé, dans son courriel 25 novembre 2019, relatives à la désignation de deux délégués suppléants.

26. La CNPD a ensuite été informée, le 19 mars 2021, de la désignation d'un nouveau DPD, à compter du 1<sup>er</sup> avril 2021, lequel était auparavant le délégué suppléant « *pour tous les traitements de données personnelles autres que ceux du département Compliance* ». Lors de l'audience du 16 juin 2021, le contrôlé a précisé que, du fait de cette désignation, le risque de conflit d'intérêts qui avait été relevé par le chef d'enquête n'existe plus, le nouveau DPD n'exerçant pas la fonction de « *Head of compliance* ».

27. Néanmoins, si des mesures ont été prises par le contrôlé dans le sens d'une mise en conformité, il convient de constater que celles-ci ont été décidées en cours d'enquête.

28. Dès lors, la formation restreinte conclut que l'article 38.6 du RGPD n'a pas été respecté par le contrôlé.

### **III. Sur les mesures correctrices**

#### **A. Les principes**

29. Conformément à l'article 12 de la loi du 1<sup>er</sup> août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale dispose des pouvoirs prévus à l'article 58.2 du RGPD :

- a) *avertir un responsable du traitement ou un sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions du présent règlement;*
- b) *rappeler à l'ordre un responsable du traitement ou un sous-traitant lorsque les opérations de traitement ont entraîné une violation des dispositions du présent règlement;*
- c) *ordonner au responsable du traitement ou au sous-traitant de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits en application du présent règlement;*
- d) *ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec les dispositions du présent règlement, le cas échéant, de manière spécifique et dans un délai déterminé;*
- e) *ordonner au responsable du traitement de communiquer à la personne concernée une violation de données à caractère personnel;*
- f) *imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement;*
- g) *ordonner la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement en application des articles 16, 17 et 18 et la notification de ces mesures aux destinataires auxquels les données à caractère personnel ont été divulguées en application de l'article 17, paragraphe 2, et de l'article 19;*
- h) *retirer une certification ou ordonner à l'organisme de certification de retirer une certification délivrée en application des articles 42 et 43, ou ordonner à l'organisme de certification de ne pas délivrer de certification si les exigences applicables à la certification ne sont pas ou plus satisfaites;*
- i) *imposer une amende administrative en application de l'article 83, en complément ou à la place des mesures visées au présent paragraphe, en fonction des caractéristiques propres à chaque cas;*
- j) *ordonner la suspension des flux de données adressés à un destinataire situé dans un pays tiers ou à une organisation internationale. »*



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

## B. En l'espèce

### 1. Quant au rappel à l'ordre

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 les articles 37.7 et 38.6 du RGPD, la formation restreinte considère qu'il est justifié de prononcer un rappel à l'ordre à son encontre.

### 2. Quant à la prise de mesures correctrices

33. Dans son courrier complémentaire à la communication des griefs du 3 août 2020, le chef d'enquête propose à la formation restreinte de prendre la mesure correctrice suivante :

*« a) Ordonner la mise en place de mesures assurant que les différentes missions et tâches, actuelles ou passées, de la personne exerçant la fonction de DPD n'entraînent pas de conflits d'intérêts conformément aux exigences de l'article 38 paragraphe 6 du RGPD. Bien que plusieurs manières puissent être mises en œuvre, une des possibilités serait l'implication d'une tierce personne, bénéficiant des compétences nécessaires, pour la revue des traitements pour lesquels il existe un conflit d'intérêt (en l'occurrence pour les traitements AML/KYC). »*

34. Quant à la mesure correctrice proposée par le chef d'enquête sous a) du point 33 de la présente décision et par référence au point 30 de la présente décision, la formation restreinte prend en compte les démarches effectuées par le contrôlé afin de se conformer aux dispositions de l'article 38.6 du RGPD. Plus particulièrement, elle prend note des faits suivants :

- En ce qui concerne la violation de l'article 38.6 du RGPD, la formation restreinte constate qu'un nouveau DPD a été désigné, à compter du 1<sup>er</sup> avril 2021, et que ce nouveau DPD n'exerce pas la fonction de « *Head of compliance* ». La formation restreinte considère dès lors qu'il n'y a pas lieu de prononcer la mesure correctrice proposée par le chef d'enquête sous a) du point 33 de la présente décision.

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

- de retenir les manquements aux articles 37.7 et 38.6 du RGPD ;
- de prononcer à l'encontre de la Société A un rappel à l'ordre au regard de la violation des articles 37.7 et 38.6 du RGPD.

Ainsi décidé à Belvaux en date du 13 octobre 2021.

La Commission nationale pour la protection des données siégeant en formation restreinte

Tine A. Larsen  
Présidente

Thierry Lallemand  
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.