

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

Délibération n° 30FR/2021 du 4 août 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^{er} 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 2016¹, 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 « l'établissement public A » établi à [...] et inscrit 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] est un [...]. Il est un établissement public [...], sous la tutelle du Ministère [...]. Le [contrôlé] a pour mission spécifique de [...].

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 27 septembre 2018. Une visite sur place a eu lieu le 31 janvier 2019 et des informations complémentaires ont été reçues par courriel en date du 5 juillet 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.



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

- 1) S'assurer que l'organisme soumis à l'obligation de désigner un DPD l'a bien fait ;
- 2) S'assurer que l'organisme a publié les coordonnées de son DPD ;
- 3) S'assurer que l'organisme a communiqué les coordonnées de son DPD à la CNPD ;
- 4) S'assurer que le DPD dispose d'une expertise et de compétences suffisantes pour s'acquitter efficacement de ses missions ;
- 5) S'assurer que les missions et les tâches du DPD n'entraînent pas de conflit d'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 7 novembre 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 du 7 novembre 2019.

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 contrôle² ;
- l'obligation de fournir les ressources nécessaires au DPD³ ;

² Objectif n°3

³ Objectif n°6



- l'obligation pour le DPD d'exercer un contrôle adéquat du traitement des données au sein de l'organisme contrôlé⁴.

8. Par courrier du 11 décembre 2019, le contrôlé a fait parvenir au chef d'enquête sa prise de position quant aux manquements énumérés dans la communication des griefs. Dans ce courrier, le contrôlé affirme d'une part qu'un plan de contrôle pour l'année 2020 « *est en cours de formalisation* » afin de pallier au troisième manquement et, d'autre part, apporte des informations complémentaires quant aux ressources allouées pour remplir les missions liées à la protection des données.

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 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 30 septembre 2020, le [contrôlé] a confirmé la bonne réception du courrier complémentaire à la communication des griefs, sans soulever de remarques supplémentaires.

11. La présidente de la formation restreinte a informé le contrôlé par courrier du 3 décembre 2020 que son affaire serait inscrite à la séance de la formation restreinte du 15 janvier 2021 et qu'il pouvait assister à cette séance. Le contrôlé a informé par courriel en date du 14 janvier 2021 qu'il ne participerait pas à ladite séance.

12. Lors de la séance de la formation restreinte du 15 janvier 2021, le chef d'enquête a exposé ses observations orales à l'appui de ses observations écrites et a répondu aux questions posées par la formation restreinte. Le contrôlé n'était pas présent lors de la séance.

⁴ Objectif n°10

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

13. 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.

14. 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* »⁵.

15. 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

16. 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.

17. Il ressort de la communication des griefs que la prise de fonction du DPD du [contrôlé] a eu lieu en mai 2018. Cependant, la communication des coordonnées du DPD à la CNPD n'a été faite que le 27 septembre 2018.

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.

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

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 à l'obligation de fournir les ressources nécessaires au DPD

1. Sur les principes

20. 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 ».

21. Il résulte des lignes directrices concernant les DPD que les aspects suivants doivent notamment être pris en considération⁶ :

- « 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 ».

⁶ WP 243 v.01, version révisée et adoptée le 5 avril 2017, p. 17

22. 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 délégué à la protection des données doit être effective et dotée de ressources adéquates au regard du traitement de données réalisé* ».

2. En l’espèce

23. Il ressort du rapport d’audit que, au vu de la taille des organismes sélectionnés dans le cadre de la campagne d’audit, 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 que le chef d’enquête s’attend également à un niveau élevé de ressources compte tenu de l’existence d’opérations de traitement complexes ou sensibles.

24. Il ressort du rapport d’enquête et de la communication des griefs que le DPD du [contrôlé] est affecté à ses missions à hauteur de 50% de son temps de travail. Cependant, en pratique, le DPD consacrait 75% de son temps à ses fonctions entre mai 2018 et mars 2019 et y consacrait encore 70% de son temps en juin 2019. En outre, le DPD bénéficiait de l’appui d’un consultant externe jusqu’en mars 2019.

25. Dans sa prise de position du 11 décembre 2019, le contrôlé énumère le nombre de traitements de données à caractère personnel effectués, à savoir :

- « [...] traitements à des fins de [...],
- [...]
- [...] projets à des fins [...]
- En tant que sous-traitants : [...] collectes de données [...]

Le contrôlé affirme que « *les traitements effectués à des fins de [...]* ».



26. La formation restreinte prend note qu'il ressort du dossier d'enquête que le DPD est également [...] du [contrôlé] et consacre, en pratique, environ 70% de son temps de travail à ses missions de DPD. Même en prenant en considération le fait que le DPD consacre plus de temps à ses missions de DPD que les 50% initialement prévus ainsi que le support fournit par l'intervention temporaire, jusqu'en mars 2019, d'un consultant externe, la formation restreinte estime que le DPD ne disposait pas du temps suffisant pour accomplir ses tâches, ceci notamment au regard de la sensibilité, de la complexité et du volume des données traitées par le contrôlé.

27. 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 à l'obligation pour le DPD d'exercer un contrôle adéquat du traitement des données au sein de l'organisme contrôlé

1. Sur les principes

28. Selon l'article 39.1 b) du RGPD, le DPD a, entre autres, la mission de « *contrôler le respect du présent règlement, d'autres dispositions du droit de l'Union ou du droit des Etats membres en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant* ». Le considérant (97) précise que le DPD devrait aider l'organisme à vérifier le respect, au niveau interne, du RGPD.

29. Il résulte des lignes directrices concernant les DPD⁷ que, dans le cadre de sa mission de contrôle, le DPD peut notamment :

- recueillir des informations permettant de recenser les activités de traitement ;
- analyser et vérifier la conformité des activités de traitement ;

⁷ WP 243 v.01, version

- informer et conseiller le responsable du traitement ou le sous-traitant et formuler des recommandations à son intention.

2. En l'espèce

30. Il ressort du rapport d'audit que, pour que le chef d'enquête considère l'objectif 10 comme atteint par le contrôlé dans le cadre de cette campagne d'audit, il s'attend à ce que « *l'organisme dispose d'un plan de contrôle formalisé en matière de protection des données (même s'il n'est pas encore exécuté)* ».

31. Selon la communication des griefs, page 3, « *il ressort de l'enquête que le [contrôlé] n'a pas de plan de contrôle formalisé, spécifique à la protection des données. Le fait que le DPD réagisse de manière ad hoc aux situations problématiques qu'il rencontre et sa collaboration avec le responsable [...] pour l'établissement d'un plan de contrôle ne saurait suffire à démontrer l'accomplissement suffisant des missions de contrôle du DPD* ».

32. La formation restreinte constate que l'article 39.1 du RGPD énumère les missions que le DPD doit au moins se voir confier, dont la mission de contrôler le respect du RGPD, sans toutefois exiger que l'organisme mette en place des mesures spécifiques pour assurer que le DPD puisse accomplir sa mission de contrôle.

33. Le rapport d'enquête précise d'ailleurs que « *le DPD réagit de manière ad hoc aux situations problématiques qu'il rencontre* » et que « *le DPD travaille par ailleurs en étroite collaboration avec la responsable [...]* ».

34. Néanmoins, il a été précisé à juste titre en page 2 de la communication des griefs (sous « remarques préliminaires ») que « *[l]es exigences du RGPD ne sont pas toujours strictement définies. Dans une telle situation, il revient aux autorités de contrôle de vérifier la proportionnalité des mesures mises en place par les responsables de traitement au regard de la sensibilité des données traitées et des risques encourus par les personnes concernées* ».

35. Or, compte tenu du fait que les activités du contrôlé impliquent des traitements de données à caractère personnel qui touchent potentiellement un nombre important de personnes

concernées, la formation restreinte considère que la mission de contrôle effectuée par le DPD auprès du contrôlé devrait être davantage formalisée, par exemple par un plan de contrôle en matière de protection des données, afin de pouvoir démontrer que le DPD puisse effectuer sa mission de contrôle du respect du RGPD de façon adéquate.

36. La formation restreinte prend note que, dans son courrier du 11 décembre 2019, le contrôlé indique qu'un plan de contrôle est en cours d'élaboration pour l'année 2020 afin de pallier à ce manquement. Néanmoins, cette décision étant intervenue en cours d'enquête, la formation restreinte se rallie au constat du chef d'enquête selon lequel le contrôlé n'a pas été en mesure de démontrer que le DPD peut exercer ses missions de contrôle du respect du RGPD.

37. La formation restreinte constate qu'elle ne dispose pas de la documentation qui permettrait de démontrer que cette mesure a été mise en place par le contrôlé.

38. Au vu de ce qui précède, la formation restreinte conclut que l'article 39.1 b) du RGPD n'a pas été respecté par le contrôlé.

III. Sur les mesures correctrices et amendes

A) Les principes

39. Conformément à l'article 12 de la loi du 1^{er} 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 adressés à un destinataire situé dans un pays tiers ou à une organisation internationale. »*

40. Conformément à l'article 48 de la loi du 1^{er} 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.

41. 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 ».

42. 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.

43. 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 et/ou de la fixation du montant d'une éventuelle amende administrative à prononcer.

B) En l'espèce

1. Quant à l'imposition d'une amende administrative

44. 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 le montant de 6.600 euros.

45. 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 de la violation (article 83.2 a) du RGPD), la formation restreinte retient des manquements par le contrôlé aux articles 37.7, 38.2 et 39.1 b) du RGPD.

- Quant à la gravité de la violation (article 83.2 a) du RGPD), la formation restreinte relève qu'en ce qui concerne le manquement aux articles 38.2 et 39.1 b) du RGPD, 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 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 de contrôle du respect du RGPD. Un manquement aux articles 38.2 et 39.1 b) 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 :
 - (1) la prise de fonction du DPD du [contrôlé] a eu lieu en mai 2018 mais que la communication des coordonnées du DPD à la CNPD n'a été faite que le 27 septembre 2018. Le manquement à l'article 37.7 du RGPD a donc duré quatre mois après l'entrée en vigueur du RGPD ;

 - (2) le contrôlé n'a pas indiqué de mesure afin de pallier au manque de ressources allouées au DPD pour lui permettre de remplir ses missions et la formation restreinte n'a pas connaissance d'un quelconque changement quant au temps de travail du DPD, de telle sorte que le manquement à l'article 38.2 du RGPD dure depuis le 25 mai 2018 ;

 - (3) le contrôlé a indiqué dans son courrier du 11 décembre 2019 qu'un plan de contrôle est en cours d'élaboration pour l'année 2020. La formation restreinte ne dispose cependant pas de la documentation qui permettrait de démontrer que cette mesure a été effectivement mise en place par le contrôlé. Le manquement à l'article 39.1 du RGPD a donc duré dans le temps, à tout le moins entre le 25 mai 2018 et décembre 2019.

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.

46. Quant au nombre de personnes concernées affectées par la violation (article 83.2 a) du RGPD), la formation restreinte relève [que] le [contrôlé] est amené à traiter un grand nombre de données à caractère personnel relatives à un grand nombre de personnes concernées. Comme avancé au point 25 de la présente décision, dans sa prise de position du 11 décembre 2019, le contrôlé précise le nombre de traitements de données à caractère personnel effectués par le contrôlé qui serait de [...] traitements à des fins de [...], [...] projets à des fins de [...] et, en tant que sous-traitant, [...] collectes de données [...], étant précisé que cette analyse constitue une indication quant à l'ampleur des activités de traitement effectuées par le contrôlé, et non pas quant au nombre de personnes dont les données à caractère personnel sont effectivement traitées par ce dernier. Il s'ensuit néanmoins que le nombre de personnes concernées par la violation est 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.
- Quant aux catégories de données à caractère personnel concernées par la violation (article 83.2 g) du RGPD), la formation restreinte tient compte du fait que le contrôlé peut être amené à traiter des [...] données sensibles au sens de l'article 9 du RGPD.

47. 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 de son montant.

48. Elle relève que si plusieurs mesures ont été décidées par le contrôlé afin de remédier en partie ou en totalité à certains manquements, celles-ci n'ont été décidées qu'à la suite du lancement de l'enquête par les agents de la CNPD en date du 17 septembre 2018.

49. 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 37.7, 38.2 et 39.1 b) du RGPD.

50. 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 37.7, 38.2 et 39.1 b) du RGPD est reproché au contrôlé, le montant maximum de l'amende pouvant être retenu s'élève à 10 millions d'euros ou 2% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

51. 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 6.600 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

52. 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 à disposition de 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 de tout ou partie de ses autres missions/fonctions ou de lui fournir un support formel et pérenne, en interne ou en externe, quant à l'exercice de ses missions de DPD.

b) Ordonner le déploiement de la mission de contrôle du DPD, conformément à l'article 39 paragraphe 1 b) du RGPD. Bien que plusieurs manières puissent être envisagées pour parvenir à ce résultat, le DPD devrait documenter ses contrôles sur l'application des règles et procédures internes en matière de protection des données (deuxième ligne de défense). Cette documentation pourrait prendre la forme d'un plan de contrôle. »

53. En ce qui concerne le manquement à l'article 38.2 du RGPD, compte tenu du fait que le contrôlé n'a fourni aucune indication à la CNPD quant à d'éventuelles mesures prises pour pallier à ce manquement, la formation restreinte considère dès lors qu'il y a lieu de prononcer la mesure correctrice proposée par le chef d'enquête et reprise sous a) du point 52 ci-avant.

54. Quant aux mesures correctrices proposées par le chef d'enquête et par référence au point 8 de la présente décision, la formation restreinte prend en compte les démarches effectuées par le contrôlé afin de se conformer à l'article 39.1 b) du RGPD, à savoir le fait que le contrôlé a indiqué dans son courrier du 11 décembre 2019 qu'il a été décidé d'élaborer un plan de contrôle pour l'année 2020.

55. Néanmoins, la formation restreinte ne dispose pas de la documentation permettant de démontrer la mise en œuvre de cette mesure de mise en conformité par le contrôlé. La formation restreinte considère dès lors qu'il y a lieu de prononcer la mesure correctrice proposée par le chef d'enquête et reprise sous b) du point 52 ci-avant.

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, 38.2 et 39.1 b) du RGPD ;

- de prononcer à l'encontre de « l'établissement public A » une amende administrative d'un montant de six mille six cents euros (6.600 euros) au regard de la violation des articles 37.7, 38.2 et 39.1 b) du RGPD ;

- de prononcer à l'encontre de « l'établissement public A » une injonction de se mettre en conformité avec l'article 38.2 du RGPD, dans un délai de quatre mois suivant la notification de la décision de la formation restreinte, en particulier :

s'assurer de la mise à disposition des ressources nécessaires au DPD afin que celui-ci dispose du temps nécessaire pour accomplir ses tâches ;

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

s'assurer que le DPD exerce, de façon formelle et documentée, sa mission de contrôle de l'application du RGPD auprès du responsable du traitement.

Ainsi décidé à Belvaux en date du 4 août 2021.

Pour 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.