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° 38FR/2021 du 15 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 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 l'établissement public A, établi à L[…], et inscrite au registre de commerce et des sociétés sous le numéro J[…] (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 établissement public […] sous la tutelle du Ministère […]. […] le contrôlé a pour mission […]

4. Par courrier du 17 septembre 2018, le chef d'enquête a envoyé un questionnaire préliminaire au contrôlé, auquel ce dernier a répondu par courrier du 5 octobre 2018. Une première visite sur place a eu lieu le 24 janvier 2019, une seconde visite sur place a eu lieu le 27 mai 2019 et des informations complémentaires ont été reçues le 23 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'intérêts ;
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 14 février 2020 (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 14 février 2020.

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

- l'obligation de publier les coordonnées du DPD[2] ;
- l'obligation de désigner le DPD sur base de ses qualités professionnelles[3] ;

[2] Objectif n°2
[3] Objectif n°4

- l'obligation d'associer le DPD à toutes les questions relatives à la protection des données à caractère personnel[4] ;
- l'obligation de fournir les ressources nécessaires au DPD[5] ;
- l'obligation de veiller à ce que les autres missions et tâches du DPD n'entraînent pas de conflit d'intérêts[6] ;
- la mission de contrôle du DPD[7].

8. Le 10 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.

9. Le contrôlé a répondu au courrier complémentaire à la communication des griefs par un courrier en date du 14 septembre 2020 dans lequel il présente ses observations pour chaque manquement retenu par le chef d'enquête.

10. En outre, le contrôlé a, en date du 28 octobre 2020, demandé l'accès au dossier d'enquête le concernant. L'accès au dossier d'enquête lui a été transmis par la Commission nationale le 9 novembre 2020.

11. La présidente de la formation restreinte a informé le contrôlé par courrier du 12 avril 2021 que son affaire serait inscrite à la séance de la formation restreinte du 16 juin 2021 et qu'il pouvait assister à cette séance. Le contrôlé a informé par courriel du 25 mai 2021 qu'il participerait à ladite séance.

12. Lors de la séance de la formation restreinte du 16 juin 2021, le chef d'enquête et le contrôlé ont présenté leurs observations orales sur l'affaire et ont répondu aux questions posées par la formation restreinte. Le contrôlé a eu la parole en dernier.

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

13. Le contrôlé a fourni des informations complémentaires par courriel du 17 juin 2021, suite à une demande en ce sens de la formation restreinte.

II. En droit

A. Sur le manquement à l'obligation de publier les coordonnées du DPD

1. Sur les principes

14. L'article 37.7 du RGPD prévoit l'obligation pour l'organisme contrôlé de publier les coordonnées du DPD. En effet, il résulte de l'article 38.4 du RGPD que les personnes concernées doivent être en mesure de pouvoir contacter le DPD au sujet de toutes questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le RGPD.

15. Les lignes directrices concernant les DPD expliquent à cet égard que cette exigence vise à garantir que « *les personnes concernées (tant à l'intérieur qu'à l'extérieur de l'organisme) puissent aisément et directement prendre contact avec le DPD sans devoir s'adresser à un autre service de l'organisme* ». Les lignes directrices précisent également que « *les coordonnées du DPD doivent contenir des informations permettant aux personnes concernées de joindre celui-ci facilement (une adresse postale, un numéro de téléphone spécifique et/ou une adresse de courrier électronique spécifique)* ».[8]

16. En outre, l'article 12.1 du RGPD dispose que le responsable du traitement doit prendre des mesures appropriées pour fournir toute information visée aux articles 13 et 14 du RGPD en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples. Parmi les informations qui doivent être transmises à la personne concernée figure l'information relative aux coordonnées du DPD, conformément aux articles 13.1.b) et 14.1.b) du RGPD.

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

2. En l'espèce

17. Il résulte du rapport d'audit que, pour que le chef d'enquête considère l'objectif 2 comme atteint par le contrôlé dans le cadre de cette campagne d'audit, le chef d'enquête s'attend à ce que l'organisme contrôlé publie les coordonnées de son DPD en interne au sein de l'organisme et en externe auprès du public qui représente les personnes concernées par le traitement. Le DPD doit pouvoir être contacté aisément et directement via un canal de communication adapté aux personnes concernées. Une communication active en interne est attendue, via notamment des emails, newsletters ou encore espaces dédiés sur l'intranet. En externe, il est au moins attendu que les coordonnées du DPD soient facilement accessibles sur le site internet de l'organisme.

18. Il ressort de la communication des griefs que, lors de la première visite des agents de la CNPD en charge de l'enquête le 24 janvier 2019, les coordonnées du DPD étaient difficiles à trouver sur le site internet du contrôlé dans la mesure où, d'une part, le site internet ne contenait pas de section dédiée à la protection des données et, d'autre part, la notice d'information relative à la protection des données n'était disponible qu'en anglais, sans traduction dans aucune des langues officielles du Luxembourg.

19. Le contrôlé a procédé à des modifications au cours de l'enquête afin de remédier à cette problématique. Il a en effet, dans un premier temps, créé une section protection des données sur son site internet et, dans un second temps, ajouté des liens permettant de télécharger des versions française et allemande de la notice d'information sous format PDF.

20. Le chef d'enquête a donc conclu dans la communication des griefs que, au cours de l'enquête, les coordonnées du DPD étaient devenues plus facilement accessibles pour les personnes concernées.

21. Toutefois, comme expliqué en page 2 de la communication des griefs, « *[l]es faits pris en compte dans le cadre de la présente [communication des griefs] sont ceux constatés au début de l'enquête. Les modifications intervenues ultérieurement, même si elles permettent finalement d'établir la conformité du responsable du traitement, ne permettent pas d'annuler un manquement constaté.* »

22. Dans ce cadre, la formation restreinte constate que le RGPD est applicable depuis le 25 mai 2018 de sorte que l'obligation de publier les coordonnées du DPD, ainsi que le principe de transparence tel qu'exposé à l'article 12.1 du RGPD, existent depuis cette date. Publier les coordonnées du DPD sur un site internet sans prendre les mesures nécessaires afin de s'assurer que les personnes concernées soient à même de trouver l'information et de la comprendre revient à vider de sens l'obligation de l'article 37.7 du RGPD.

23. 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 désigner le DPD sur base de ses qualités professionnelles

1. Sur les principes

24. 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 […]* ».

25. Aux termes du 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* ».

26. Par ailleurs, les lignes directrices du Groupe de travail « Article 29 » concernant les DPD 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* »[9] et qu'« *il est nécessaire que les DPD disposent d'une expertise dans le domaine des législations et pratiques nationales et*

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

européennes en matière de protection des données, ainsi que d'une connaissance approfondie du RGPD »[10].

27. Les lignes directrices concernant les DPD indiquent ensuite 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* »[11].

2. <u>En l'espèce</u>

28. Il résulte du rapport d'audit que, dans le cadre de cette campagne d'audit, pour que le chef d'enquête considère l'objectif 4 comme atteint par le contrôlé, le chef d'enquête s'attend à ce que le DPD ait au minimum trois ans d'expérience professionnelle en matière de protection des données.

29. Selon la communication des griefs, page 3, à la date du lancement de l'audit, un DPD externe était en fonction et « *[c]elui-ci possédait toutes les compétences requises en matière juridique (avocat inscrit au Barreau de Luxembourg) et de protection des données (certificat CIPP/E)* ».

30. Un nouveau DPD interne a cependant été nommé au cours de l'enquête, en avril 2019. Selon la communication des griefs, page 3, ce nouveau DPD interne « *est également responsable […] et il dispose de la connaissance du domaine et de la structure. Néanmoins, il convient de constater qu'il n'a pas de formation initiale en matière juridique, de protection des données et informatique, ni ne justifie d'une pratique antérieure en la matière* ».

31. Dans sa prise de position du 14 septembre 2020, le contrôlé a tenu à souligner les difficultés auxquelles il a dû faire face pour recruter un DPD au profil adapté, à savoir une personne expérimentée et ayant des connaissances sur le fonctionnement du secteur de […]. Le conseil d'administration du contrôlé qualifie le premier recrutement externe de *« tentative*

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

échouée » et a choisi de désigner en tant que DPD un employé interne expérimenté et à même de comprendre les enjeux du secteur de […] et la complexité réglementaire qui le caractérise. Le contrôlé considère que cette connaissance du métier est un critère important et prioritaire au regard de son secteur spécifique.

Le contrôlé ajoute que le nouveau DPD interne a suivi plusieurs formations en matière de protection des données entre 2017 et 2019, qu'un coaching régulier hebdomadaire avec l'assistance d'un cabinet d'avocats spécialisé en matière de protection des données était en place depuis avril 2019 et que le DPD participe mensuellement depuis décembre 2018 aux sessions du groupe de travail informel du secteur public […].

En outre, le DPD a la possibilité de s'appuyer quotidiennement, pour l'exécution de ses missions, sur la contribution des équipes […] et, sur le service informatique, sur le service juridique, sur l'expert en gestion des risques et sur toute autre ressource interne jugée utile. Depuis septembre 2017, le contrôlé a mis en place des « *GDRP points of contacts* », consistant en la désignation de quelques personnes appartenant aux différents corps de métiers du contrôlé pour être le relais du DPD[12].

32. La formation restreinte prend note que, selon le chef d'enquête, les formations relatives à la protection des données auxquelles le DPD interne a assisté depuis sa désignation, ainsi que le fait qu'il ait accès à un certain nombre de supports internes et externes dans l'exécution de ses missions, ne sauraient suffire à établir, au moment de la désignation du nouveau DPD interne, l'existence d'une expertise suffisante et adaptée aux besoins du contrôlé en matière de protection des données[13].

33. Toutefois, comme cela est relevé en page 2 de la communication des griefs, « *[l]es faits pris en compte dans le cadre de la présente sont ceux constatés au début de l'enquête* ».

34. Or, la formation restreinte constate qu'au début de l'enquête, un DPD externe était en fonction et, comme cela a été relevé par le chef d'enquête et repris au point 29 de la présente

[12] Compte-rendu de la visite du 24 janvier 2019, page 3
[13] Communication des griefs, page 3.

décision, celui-ci possédait toutes les compétences requises en matière juridique et en matière de protection des données.

35. Au vu de ce qui précède, la formation restreinte conclut qu'il n'y a pas lieu de retenir un manquement à l'article 37.5 du RGPD.

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

36. 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.

37. 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].

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

- inviter le DPD à participer régulièrement aux réunions de l'encadrement supérieur et intermédiaire ;
- recommander la présence du DPD lorsque des décisions ayant des implications en matière de protection des données sont prises ;

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

- prendre toujours dûment en considération l'avis du DPD ;
- consulter immédiatement le DPD lorsqu'une violation de données ou un autre incident se produit.

39. En outre, 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 traitements dans lesquels le DPD doit être consulté.

2. <u>En l'espèce</u>

40. Il ressort du rapport d'audit que, pour que le chef d'enquête considère l'objectif 8 comme rempli par le contrôlé dans le cadre de cette campagne d'audit, il s'attend à ce que le DPD participe de manière formalisée et sur base d'une fréquence définie au Comité de Direction, aux comités de coordination de projet, aux comités de nouveaux produits, aux comités sécurité ou tout autre comité jugé utile dans le cadre de la protection des données.

41. Selon la communication des griefs, page 4, le DPD externe qui était en fonction au début de l'audit avait un rôle qualifié d'essentiellement « *réactif* ». *« [Son] implication était donc relativement limitée. Il intervenait principalement sur demande explicite du responsable du traitement et non de manière spontanée* ». Le rapport d'audit, page 9, précise que l'implication limitée du DPD externe se caractérisait plus particulièrement par une « *participation faible aux réunions récurrentes, uniquement sur invitation quand le besoin a été estimé* ».

42. Dans sa prise de position du 14 septembre 2020, page 6, le contrôlé estime que la description par le chef d'enquête du rôle essentiellement réactif du DPD externe en fonction au début de l'enquête est inexacte et revient à minimiser l'implication du DPD externe, comme en atteste le relevé des heures prestées sur plusieurs projets […].

43. Le nouveau DPD interne, quant à lui, participe plus aisément aux différentes réunions de projets. La remontée d'informations est facilitée par la proximité et les différents relais en place dans la structure. En outre, d'après le rapport d'audit, page 9, le DPD interne est un invité permanent du comité exécutif du contrôlé (fréquence toutes les deux semaines) et un point

systématique « GDPR » est dans l'agenda de chaque conseil d'administration qui a lieu tous les trois mois.

Cependant, d'après le rapport d'audit, page 9, un circuit précis concernant les avis à rendre par le DPD n'est pas encore clairement défini, en raison de la désignation récente du DPD interne.

44. Dans sa prise de position du 14 septembre 2020, le contrôlé informe la CNPD quant à la mise en place d'un processus interne ([…]) afin de formaliser et documenter l'association du DPD aux questions relatives à la protection des données. Ce processus interne est mis en œuvre systématiquement pour chaque nouvelle activité […] du contrôlé et vise à permettre :

- une documentation préalable et une remontée d'informations systématique au DPD avant la mise en œuvre des traitements du contrôlé, et ce au plus tard au moment de la mise en place des contrats,
- l'identification en amont des points de protection des données sensibles,
- la revue en amont des notices d'information et formulaires de consentement distribués […],
- une sensibilisation des équipes opérationnelles et des échanges avec ces dernières, dans une optique de *privacy by design*, et
- la planification ou la réalisation d'analyses d'impact sur la protection des données.

45. Le contrôlé précise également que l'association du DPD aux questions de protection des données s'effectue aussi à l'initiative des équipes ou du DPD lui-même dans le cadre de la revue documentaire, la co-signature des contrats relatifs à la protection des données, la conception des projets […] du contrôlé, l'assistance des équipes internes dans la réalisation des analyses d'impact et la participation du DPD au comité exécutif en tant qu'invité permanent.

46. La formation restreinte prend note de la mise en place par le contrôlé d'un processus interne de formalisation et documentation de l'implication du nouveau DPD interne aux questions relatives à la protection des données. Si ces mesures devraient faciliter l'association du DPD interne à toutes les questions relatives à la protection des données, il convient néanmoins de constater que celles-ci ont été décidées en cours d'enquête.

47. En effet, comme expliqué en page 2 de la communication des griefs, « *[l]es faits pris en compte dans le cadre de la présente [communication des griefs] sont ceux constatés au début de l'enquête. Les modifications intervenues ultérieurement, même si elles permettent finalement d'établir la conformité du responsable du traitement, ne permettent pas d'annuler un manquement constaté.* »

48. La formation restreinte est d'avis que le contrôlé n'a pas démontré avec suffisance l'association du DPD externe, en fonction au début de l'enquête, d'une manière appropriée et en temps utile à toutes les questions relatives à la protection des données.

49. Par conséquent, la formation restreinte se rallie au constat du chef d'enquête selon lequel, au début de l'enquête, le responsable du traitement n'a pas été en mesure de démontrer que le DPD externe était associé de manière appropriée à toutes les questions relatives à la protection des données à caractère personnel.

50. Au vu de ce qui précède, la formation restreinte conclut que l'article 38.1 du RGPD n'a pas été respecté.

D. Sur le manquement relatif à la mission de contrôle du DPD

1. Sur les principes

51. 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 et des règles internes du responsable du traitement ou du sous-traitant 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.

52. Il résulte des lignes directrices concernant les DPD[15] que le DPD peut, dans le cadre de ses tâches de contrôle, notamment :

- recueillir des informations permettant de recenser les activités de traitement ;
- analyser et vérifier la conformité des activités de traitement ;
- informer et conseiller le responsable du traitement ou le sous-traitant et formuler des recommandations à son intention.

2. <u>En l'espèce</u>

53. Il ressort du rapport d'audit que, pour qu'il puisse considérer l'objectif 10 comme rempli par le contrôlé dans le cadre de cette campagne d'audit, le chef d'enquête 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)* ».

54. Selon la communication des griefs, page 5, « *il ressort de l'enquête que l'organisme ne dispose pas de contrôles formalisés spécifiques à la protection des données. Dans une logique de gestion quotidienne de la protection des données, et compte tenu du volume de données traitées et de la sensibilité de certaines de ces données (voir remarques préliminaires), il est attendu que les missions de contrôle du DPD soient mieux formalisées, par exemple avec l'instauration d'un plan de contrôle* ».

55. Dans sa prise de position du 14 septembre 2020, le contrôlé indique que le contrôle de la conformité du responsable du traitement au RGPD est assuré grâce à la mise en place des moyens suivants :

- la revue juridique du registre des traitements du contrôlé par un cabinet d'avocats spécialisés en protection des données, de janvier à octobre 2019,
- un audit interne sous-traité à un cabinet d'audit portant sur des aspects organisationnels,
- un audit externe réalisé par un cabinet d'audit, en vue d'évaluer la conformité du contrôlé […].

[15] WP 243 v.01, version révisée et adoptée le 5 avril 2017, page 20

56. 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. Les lignes directrices concernant les DPD indiquent notamment que la tenue du registre des activités de traitement visé à l'article 30 du RGPD peut être confiée au DPD et que « *ce registre doit être considéré comme l'un des outils permettant au DPD d'exercer ses missions de contrôle du respect du RGPD, ainsi que d'information et de conseil du responsable du traitement et du sous-traitant*[16] ».

57. En outre, la formation restreinte relève qu'il est précisé à juste titre en page 2 de la communication des griefs (sous « remarques préliminaires ») que « *les 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 du traitement au regard de la sensibilité des données traitées et des risques encourus par les personnes concernées* ».

58. Dans ce cadre, la formation restreinte est d'avis qu'il est possible pour un organisme de faire appel à des prestataires externes pour vérifier sa conformité au RGPD. Cependant, cet appel à des prestataires externes doit être formalisé, et cela ne doit pas avoir pour conséquence de retirer totalement cette mission de la fonction de DPD. En effet, le DPD de l'organisme doit remplir sa mission de contrôle de respect du RGPD en participant à la formalisation d'un plan de contrôle et en étant associé à l'exercice dudit contrôle par les prestataires externes, notamment en accompagnant les travaux effectués, pour ensuite être en mesure de remplir en connaissance de cause sa mission de conseil et d'information conformément à l'article 39.1 a) du RGPD.

59. En l'espèce, le contrôlé n'a pas démontré que, au début de l'enquête, un plan de contrôle du respect du RGPD aurait été formalisé ni que le DPD externe alors en fonction était associé au contrôle effectué par les prestataires externes. Par conséquent, la formation restreinte est d'avis que le contrôlé ne démontre pas avec suffisance que le DPD externe en fonction au début de l'enquête remplissait cette mission de contrôle attendue par l'article 39.1 b) du RGPD.

[16] WP 243 v.01, version révisée et adoptée le 5 avril 2017, page 22

60. 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.

E. Sur le manquement à l'obligation de fournir les ressources nécessaires au DPD

1. Sur les principes

61. 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* ».

62. Il résulte des lignes directrices concernant les DPD que les aspects suivants doivent notamment être pris en considération[17] :

- « *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* ».

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

63. Les lignes directrices concernant les DPD précisent que « *[d]'une manière générale, plus les opérations de traitement sont complexes ou sensibles, plus les ressources octroyées au DPD devront être importantes. La fonction de protection des données doit être effective et dotée de ressources adéquates au regard du traitement de données réalisé* ».

2. <u>En l'espèce</u>

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

65. D'après le rapport d'audit, le DPD externe en fonction au début de l'enquête avait un rôle essentiellement « réactif ». Les relevés d'heures de celui-ci oscillent entre 20 heures et 108 heures par mois, soit entre 0.125 ETP et 0.7 ETP.

66. La répartition mensuelle de ces heures prestées par le DPD externe est détaillée dans le compte-rendu de la visite sur place du 27 mai 2019, page 2, de la façon suivante : 20 heures en septembre 2018, 53 heures en octobre 2018, 57.2 heures en novembre 2018, 50.4 heures en décembre 2018, 122.2 heures en janvier 2019, 103.9 heures en février 2019 et 108.6 heures en mars 2019. La formation restreinte relève que cela fait donc une moyenne de 73.6 heures prestées par mois sur cette période de 7 mois, soit un ETP moyen mensuel de 0.46.

67. Au regard de ces éléments, la formation restreinte comprend que le DPD externe a commencé à prester des heures dans le cadre de ses missions qu'à partir du mois de septembre 2018. En outre, l'essentiel de ses heures ont été prestées entre janvier et mars 2019.

68. Or, la formation restreinte rappelle que le RGPD est entrée en vigueur le 25 mai 2018. C'est donc dès mai 2018 que l'organisme contrôlé avait pour obligation de respecter le RGPD en désignant un DPD exerçant sa fonction de façon effective et efficace.

69. Le rapport d'audit indique que le nouveau DPD interne a estimé quant à lui son temps de travail sur les questions de protection des données à plus de 70% par rapport à l'ensemble de ses tâches. Il est également précisé qu'un soutien juridique par un cabinet externe a été obtenu à raison d'un jour par semaine, l'unique compétence juridique du contrôlé ne pouvant apporter qu'un soutien limité au DPD interne. Le contrôlé a bénéficié également d'une assistance par un cabinet d'audit dans la conduite de la feuille de route « GDPR » du contrôlé.

70. Dans la communication des griefs, page 4, le chef d'enquête précise que « *compte tenu de l'existence d'opérations de traitement complexes ou sensibles (voir remarques préliminaires), il est attendu un niveau élevé de ressources* ». Or, le chef d'enquête relève que « *le nouveau DPD [interne], qui occupe également la fonction de responsable […] pour [le contrôlé], a évalué le temps consacré à ses fonctions de DPD à plus de 70%* » et que « *le responsable du traitement n'a pas été en mesure de démontrer l'accomplissement des missions de contrôle. Cette constatation est de nature à mettre en évidence une inadéquation entre les ressources et moyens mis à disposition du DPD et les besoins du responsable du traitement* ».

71. Dans sa prise de position du 14 septembre 2020, le contrôlé indique que le nouveau DPD interne, également responsable […] au moment de sa désignation, est *désormais Head of Compliance […]*, assisté de quatre autres personnes pour la gestion des responsabilités liées à la conformité et à la gestion des risques. D'après le contrôlé, la présence de ces quatre autres personnes permet au *Head of Compliance* […] de se concentrer sur les fonctions de DPD.

72. En outre, pour permettre au *Head of Compliance […]* d'endosser le rôle de DPD interne, le contrôlé a mis à sa disposition un budget permettant de recourir à un support externe juridique et technique adéquat.

73. Enfin, comme relevé au point 55 de la présente décision, le contrôlé indique dans sa prise de position du 14 septembre 2020, que la mission de contrôle du respect du RGPD par le contrôlé est effectuée grâce à l'aide de prestataires externes tels que des cabinets d'audit et d'avocats spécialisés. Le contrôlé est d'avis que la mission de contrôle prévue à l'article 39.1 b) du RGPD est assurée et donc que les ressources et moyens prévus aux fins d'un tel contrôle sont adaptées aux besoins du contrôlé.

74. La formation restreinte rappelle que, comme cela a été indiqué dans la communication des griefs, page 2, et déjà relevé au point 21 de la présente décision, *« [l]es faits pris en compte dans le cadre de la présente [enquête] sont ceux constatés au début de l'enquête. Les modifications intervenues ultérieurement, même si elles permettent finalement d'établir la conformité du responsable du traitement, ne permettent pas d'annuler un manquement constaté.* »

75. En outre, la formation restreinte se rallie au constat du chef d'enquête selon lequel « *compte tenu de l'existence d'opérations de traitement complexes ou sensibles (voir remarques préliminaires), il est attendu un niveau élevé de ressources* » et que « *le responsable du traitement n'a pas été en mesure de démontrer l'accomplissement des missions de contrôle. Cette constatation est de nature à mettre en évidence une inadéquation entre les ressources et moyens mis à disposition du DPD et les besoins du responsable du traitement* ».

76. Par conséquent, la formation restreinte est d'avis que le contrôlé n'a pas su démontrer avec suffisance que le contrôlé a fourni au DPD externe en fonction au début de l'enquête les ressources nécessaires pour lui permettre d'exercer ses missions.

77. 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.

F. Sur le manquement 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

78. 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* ».

79. Les lignes directrices concernant les DPD[18] 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, *« en 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 conflits 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 à l'extérieur* ».

2. <u>En l'espèce</u>

80. 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

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

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.

81. D'après la communication des griefs, page 5, « *[l]e DPD qui était en fonction au début de l'audit était externe et avocat. Il existe un principe de gestion des conflits d'intérêts.* »

82. Le nouveau DPD ensuite désigné en interne exerçait également la fonction de responsable […]. La communication des griefs relève que *« de possibles conflits d'intérêts sont susceptibles d'exister aux vues des tâches effectuées pour les deux postes. Sur base des commentaires du DPD en date du 12/08/2019, il existe au [sein du contrôlé] une politique de gestion des conflits d'intérêts potentiels. Cependant, l'analyse de conflits d'intérêts entre deux fonctions exercées par la même personne au sein du même [établissement public] n'est pas prévue. Il n'existe donc pas d'analyse des potentiels conflits d'intérêts entre la fonction de DPD et celle de responsable […]. Sur base des commentaires du DPD en date du 12/08/2019, le [contrôlé] veillera à clarifier les différentes fiches de fonction concernant la gestion des aspects liés à la protection des données afin de distinguer plus clairement les autorités, responsabilités et missions* ».

83. Dans sa prise de position du 14 septembre 2020, le contrôlé indique que le DPD interne est désormais *Head of Compliance […]* de l'organisme. Il précise également que les fiches de fonctions *Head of Compliance* et *Risk Manager* ont été modifiées de manière à y faire apparaître plus clairement les responsabilités et missions liées à la protection des données.

84. La politique de conflits d'intérêts du contrôlé a également été mise à jour en juillet 2020, afin d'y introduire une obligation d'analyser les risques de conflit d'intérêts en présence d'un cumul de fonctions et de les faire arbitrer par le Conseil d'Administration du contrôlé.

85. Le contrôlé soutient également que l'externalisation de plusieurs aspects du contrôle de la conformité mis en œuvre jusqu'à ce jour permet au contrôlé d'écarter le risque de conflits d'intérêts s'agissant du contrôle des processus liés à la gestion […]. En effet, plusieurs aspects

du contrôle de la conformité des traitements du contrôlé (en particulier ceux mis en œuvre dans le cadre de l'exercice de la fonction *Compliance*) ont été confiés à des prestataires externes, comme soulevé au point 55 de la présente décision.

86. Par courriel en date du 17 juin 2021, le contrôlé a transmis à la formation restreinte la politique de conflits d'intérêts telle que mise à jour en juillet 2020.

87. La formation restreinte rappelle que, comme cela est indiqué en page 2 de la communication des griefs et déjà relevé au point 33 de la présente décision, « *[l]es faits pris en compte dans le cadre de la présente [enquête] sont ceux constatés au début de l'enquête* ».

88. La formation restreinte relève que, au début de l'enquête, le DPD en fonction était un DPD externe qui exerçait le métier d'avocat au sein du Barreau de Luxembourg. Les principes déontologiques auxquels sont soumis les avocats du Barreau de Luxembourg comprennent le principe selon lequel un avocat ne peut représenter ou assister des parties ayant des intérêts opposés, ni représenter ou assister un client en cas de conflit avec les intérêts personnel de l'avocat lui-même.[19] Ce principe déontologique est applicable à tout avocat inscrit au Barreau de Luxembourg en vertu de la loi modifiée du 10 août 1991 sur la profession d'avocat et le Règlement Intérieur de l'Ordre des Avocats du Barreau de Luxembourg tel qu'adopté par le Conseil de l'Ordre en date du 10 janvier 2013, sans qu'il n'y ait une obligation dans le chef des clients de vérifier le bon respect par l'avocat de ce principe.

89. Par conséquent, la CNPD est d'avis qu'il ne revenait pas au responsable du traitement de procéder à une vérification auprès de son DPD externe afin de s'assurer de l'absence de conflit d'intérêts potentiel avec d'autres clients et/ou sous-traitants du contrôlé, mais qu'au contraire, cette obligation incombait au DPD externe en application de la loi modifiée du 10 août 1991 sur la profession d'avocat et des règles déontologiques.

90. Au vu de ce qui précède, la formation restreinte conclut qu'il n'y a pas lieu de retenir un manquement à l'article 38.6 du RGPD.

[19] Site internet du Barreau de Luxembourg, Le métier d'avocat, La déontologie : https://www.barreau.lu/le-metier-d-avocat/la-deontologie

III. Sur les mesures correctrices et l'amende

A. Les principes

91. 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 58.2 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.* »

92. 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 des 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* ».

93. 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.

94. 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 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

95. Dans son courrier complémentaire à la communication des griefs du 10 août 2020, le chef d'enquête propose à la formation restreinte de prononcer à l'encontre du contrôlé une amende administrative portant sur le montant de 27.100 euros.

96. Afin de décider s'il y a lieu d'imposer une amende administrative et pour décider, le cas échéant, du montant de cette amende, la formation restreinte analyse les critères posés par l'article 83.2 du RGPD :

- Quant à la nature et la gravité de la violation [article 83.2 a) du RGPD], en ce qui concerne les manquements aux articles 37.7, 38.1, 38.2 et 39.1 b) du RGPD, la formation restreinte relève que la nomination d'un DPD par un organisme ne saurait être efficiente et efficace, à savoir faciliter le respect du RGPD par l'organisme, que dans le cas où les personnes concernées ont la possibilité de trouver facilement les coordonnées du DPD pour exercer leurs droits à la protection des données, ainsi que dans le cas où le DPD dispose des ressources nécessaires pour l'exercice de ses missions, est associé à toutes les questions relatives à la protection des données et exerce de façon effective ses missions, dont la mission de contrôle du respect du RGPD.

- Quant au critère de durée [article 83.2 a) du RGPD], la formation restreinte relève que :

  (1) le contrôlé a procédé à la modification de son site internet au cours de l'enquête afin de rendre les coordonnées du DPD plus facilement accessibles pour les personnes concernées. Une traduction en français et allemand ont notamment été ajoutées au site internet de l'audité en août 2019. Le manquement à l'article 37.7 du RGPD a donc duré dans le temps, à tout le moins entre le 25 mai 2018 et le mois d'août 2019.

  (2) le contrôlé a informé la CNPD, dans sa prise de position du 14 septembre 2020, de la mise en place d'un processus interne de formalisation et documentation de

l'implication du nouveau DPD interne aux questions relatives à la protection des données ([…]) à partir du 17 octobre 2019. Ces mesures ont néanmoins été décidées en cours d'enquête. Le manquement à l'article 38.1 du RGPD a donc duré dans le temps, à tout le moins entre le 25 mai 2018 au 19 octobre 2019.

(3) il n'a pas été démontré par le contrôlé que le DPD externe en fonction au moment de l'ouverture de l'enquête disposait des ressources nécessaires pour l'exercice de ses missions et que, d'après le rapport d'audit, le nouveau DPD interne estime son temps de travail sur les questions de protections des données à environs 70% par rapport à ses autres tâches. Le manquement à l'article 38.2 du RGPD a donc duré dans le temps, à partir du 25 mai 2018, étant précisé que la formation restreinte n'a pas pu constater que le manquement a pris fin.

(4) il n'a pas été démontré par le contrôlé que tant le DPD externe en fonction au début de l'enquête que le nouveau DPD interne ont rempli leur mission de contrôle de la conformité de l'organisme au RGPD dans le cadre de leurs fonctions quotidiennes, le contrôlé ayant choisi de faire appel à des prestataires externes, sans que ne soit démontré l'implication des DPD externe et interne dans l'organisation des travaux de contrôle. Le manquement à l'article 39.1 b) du RGPD a donc duré dans le temps, à partir du 25 mai 2018, étant précisé que la formation restreinte n'a pas pu constater que le manquement a pris fin.

- 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 traite des catégories particulières de données à caractère personnel[…].

97. La formation restreinte constate que les autres critères de l'article 83.2 du RGPD ne sont ni pertinents, ni susceptibles d'influer sur sa décision quant à l'imposition d'une amende administrative et son montant.

98. La formation restreinte relève que si plusieurs mesures ont été décidées par le contrôlé afin de remédier en totalité ou en partie à certains manquements, celle-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 (voir aussi le point 93 de la présente décision).

99. 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 manquements aux articles 37.7, 38.1, 38.2 et 39.1 b) du RGPD.

100. 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, 38.1, 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.

101. Au regard des critères pertinents de l'article 83.2 du RGPD évoqués ci-avant, la formation restreinte considère que le prononcé d'une amende de 18.000 euros apparaît à la fois effectif, proportionné et dissuasif, conformément aux exigences de l'article 83.1 du RGPD.

2. <u>Quant à la prise de mesures correctrices</u>

102. Dans son courrier complémentaire à la communication des griefs du 10 août 2020, le chef d'enquête propose à la formation restreinte de prendre les mesures correctrices suivantes :

> « *a) Ordonner la mise en place de mesures permettant au DPD (ou une équipe « Data Protection » dédiée) d'acquérir l'expertise suffisante et adaptée aux besoins du responsable du 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. Bien que plusieurs manières puissent être envisagées pour parvenir à ce résultat, une des possibilités pourrait consister à fournir un support formel interne ou externe en matière de compétences informatiques à votre DPD, et à l'inscrire à des formations accélérées/intensives en matière de protection des données. Les mesures évoquées par le responsable du traitement lors de l'audit, telles que l'accès à une expertise externe pour tout besoin d'assistance juridique, devraient être maintenues, voire même renforcées, au vue de la sensibilité des données traitées ;

b) Ordonner la mise en place de mesures assurant l'association formalisée et documentée du DPD à toutes les questions relatives à la protection des données conformément aux exigences de l'article 38 paragraphe 1 du RGPD et du principe d'« accountability ». Bien que plusieurs manières puissent être envisagées pour parvenir à ce résultat, une des possibilités pourrait être d'analyser, avec le DPD, tous les comités/groupes de travail pertinents au regard de la protection des données et de formaliser les modalités de son intervention (information antérieure de l'agenda des réunions, invitation, fréquence, statut de membre permanent, etc.) ;

c) Ordonner la mise en place de mesures garantissant des ressources nécessaires au DPD conformément aux exigences de l'article 38 paragraphe 2 du RGPD. Bien que plusieurs manières puissent être envisagées pour parvenir à ce résultat, une des possibilités pourrait être de décharger le DPD de tout ou partie de ses autres missions/fonctions ou de lui fournir du support, en interne ou en externe, quant à l'exercice de ses missions de DPD ;

d) 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 seraient l'implication d'une tierce personne, bénéficiant des compétences nécessaires ; pour la revue des traitements pour lesquels il existe un risque de conflit d'intérêt (revue de la

gestion des risques, revue des processus concernant les différents traitements présents, revue des fiches de fonctions et/ou fiche de poste ...) ;

e) Ordonner le déploiement formel et documenté de la mission de contrôle du DPD conformément à l'article 39 paragraphe 1 b) du RGPD et du principe d'« accountability ». Le DPD doit exercer ses missions de contrôle, 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 toujours 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 suivi de rapports. »

103. Quant aux mesures correctrices proposées par le chef d'enquête et par référence au point 102 de la présente décision, la formation restreinte prend en compte les démarches effectuées par le contrôlé afin de se conformer aux dispositions des articles 37.5, 38.1, 38.2, 38.6 et 39.1 b) du RGPD, notamment les mesures décrites dans son courrier du 14 septembre 2020. Plus particulièrement, elle prend note des faits suivants :

- En ce qui concerne le respect par le contrôlé de l'article 37.5 du RGPD, la formation restreinte constate que, suite à la désignation du nouveau DPD interne, celui-ci a suivi plusieurs formations en matière de protection des données de façon à ce qu'il dispose d'une expertise suffisante pour remplir ses fonctions. Cependant, comme cela a été relevé au point 35 de la présente décision, la formation restreinte considère qu'il n'y a pas lieu de retenir un manquement à l'article 37.5 du RGPD au regard de la situation du contrôlé au début de l'enquête. Par conséquent, la formation restreinte ne prononce pas la mesure correctrice telle que proposée par le chef d'enquête et reprise sous a) du point 102 de la présente décision.

- En ce qui concerne la violation de l'article 38.1 du RGPD, le contrôlé indique dans son courrier du 14 septembre 2020 qu'un processus interne de formalisation et documentation de l'implication du nouveau DPD interne aux questions relatives à la protection des données […]) a été mis en place par le contrôlé. La formation restreinte considère dès

lors qu'il n'y pas lieu de prononcer la mesure correctrice proposée par le chef d'enquête et reprise sous b) du point 102 de la présente décision.

- En ce qui concerne la violation de l'article 38.2 du RGPD, le DPD interne actuellement en fonction a estimé son temps de travail sur les questions de protection des données à environ 70% par rapport à ses autres tâches. Compte tenu du fait que le contrôlé traite un nombre substantiel de données dont le degré de sensibilité peut être relativement élevé, la formation restreinte considère que le DPD devrait disposer de ressources plus élevées pour l'exercice de ses missions. 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 c) du point 102 de la présente décision.

- En ce qui concerne le respect par l'organisme de l'article 38.6 du RGPD, la formation restreinte considère que le contrôlé n'a pas démontré que, malgré le cumul des fonctions de DPD interne et de *Head of Compliance […]*, des mesures internes suffisantes auraient été prises afin d'éviter que le DPD ne sera pas amené à se prononcer sur des traitements dont il aurait contribué à déterminer les finalités et les moyens. Cependant, comme cela a été relevé au point 90 de la présente décision, la formation restreinte considère qu'il n'y a pas lieu de retenir un manquement à l'article 38.6 du RGPD au regard de la situation du contrôlé au début de l'enquête. Par conséquent, la formation restreinte ne prononce pas la mesure correctrice telle que proposée par le chef d'enquête et reprise sous d) du point 102 de la présente décision.

- En ce qui concerne la violation de l'article 39.1 b) du RGPD, la formation restreinte est d'avis que le contrôlé n'a pas démontré que le DPD actuellement en fonction remplit sa mission de contrôle du respect du RGPD par le contrôlé, ce dernier ayant choisi de faire appel à des prestataires externes pour assurer ce contrôle, sans que ne soit démontrée l'implication du nouveau DPD interne dans l'organisation de ces travaux de contrôle. 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 e) du point 102 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, 38.1, 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 dix-huit mille euros (18.000 euros) au regard de la violation des articles 37.7, 38.1, 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 six mois suivant la notification de la décision de la formation restreinte, en particulier :

  s'assurer que le DPD dispose des ressources nécessaires pour l'exercice de ses missions ;

- 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 six mois suivant la notification de la décision de la formation restreinte, en particulier :

  s'assurer du déploiement formel et documenté de la mission de contrôle du DPD.

Ainsi décidé à Belvaux, en date du 15 octobre 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.