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

Délibération n° 41FR/2021 du 27 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, point 2;

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

Considérant ce qui suit :

I. Faits et procédure

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

[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.

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

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

3. […] le contrôlé a pour objet toutes activités relevant des banques ou établissements de crédit […].

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 28 septembre 2018. Une visite sur place a eu lieu le 29 janvier 2019. Suite à ces échanges, le chef d'enquête a établi le rapport d'audit n°[…] (ci-après : le « rapport d'audit »).

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

1) S'assurer que l'organisme soumis à l'obligation de désigner un DPD l'a bien fait ;
2) S'assurer que l'organisme a publié les coordonnées de son DPD ;
3) S'assurer que l'organisme a communiqué les coordonnées de son DPD à la CNPD ;
4) S'assurer que le DPD dispose d'une expertise et de compétences suffisantes pour s'acquitter efficacement de ses missions ;
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 21 octobre 2019 (ci-après : la « communication des griefs »), le chef d'enquête a informé le contrôlé des manquements aux obligations prévues par le RGPD qu'il a relevés lors de son enquête. Le rapport d'audit était joint audit courrier.

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

- l'obligation de publier les coordonnées du DPD[2] ;
- l'obligation d'associer le DPD à toutes les questions relatives à la protection des données[3] ;
- l'obligation de garantir l'autonomie du DPD[4] ;
- la mission de contrôle du DPD[5].

8. Par courrier du 15 novembre 2019, le contrôlé a adressé au chef d'enquête sa prise de position quant aux manquements relevés dans la communication des griefs.

9. Le 3 août 2020, le chef d'enquête a adressé au contrôlé un courrier complémentaire à la communication des griefs par lequel il informe le contrôlé sur les mesures correctrices qu'il propose à la Commission nationale siégeant en formation restreinte (ci-après : la « formation restreinte ») d'adopter. Dans ce courrier, le chef d'enquête a proposé à la formation restreinte d'adopter 4 mesures correctrices différentes ainsi que d'infliger au contrôlé une amende administrative d'un montant de 18.700 euros.

[2] Objectif n°2
[3] Objectif n°8
[4] Objectif n°7
[5] Objectif n°10

10. Par courrier du 8 septembre 2020, le contrôlé a fait parvenir au chef d'enquête ses observations quant au courrier complémentaire à la communication des griefs.

11. L'affaire a été à l'ordre du jour de la séance de la formation restreinte du 31 mai 2021. Conformément à l'article 10.2. b) du règlement d'ordre intérieur de la Commission nationale, le chef d'enquête et le contrôlé ont présenté des observations orales sur l'affaire et ont répondu aux questions posées par la formation restreinte. Le contrôlé a eu la parole en dernier.

II. En droit

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

1. Sur les principes

12. 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 les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le RGPD.

13. 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)* ».[6]

14. 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.

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

2. En l'espèce

15. Il ressort du rapport d'audit que, pour que le chef d'enquête considère l'objectif 2 comme rempli par le contrôlé dans le cadre de cette campagne d'audit, il s'attend à ce que l'organisme publie les coordonnées de son DPD en interne au sein de l'organisme et en externe auprès du public. Le DPD doit pouvoir être contacté aisément et directement via un canal de communication adapté aux personnes concernées. Dans le cadre de cette campagne d'audit, une communication active en interne est attendue, via notamment des emails, newsletters, 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.

16. D'après la communication des griefs, page 2 : « *Il ressort de l'enquête que le site web public de la Société A n'indique pas les coordonnées directes du DPD. En cas de questions ou de demandes des personnes concernées, le site web met à disposition un formulaire à compléter et à renvoyer à une adresse email générique ([…]) ou par courrier à l'adresse de la hotline […] ou via la messagerie sécurisée de […].* »

17. Le chef d'enquête en conclut que « l*es personnes concernées externes à la Société A ne peuvent pas directement prendre contact avec le DPD sans devoir s'adresser à un autre service de l'organisme.* »

18. Dans sa prise de position du 15 novembre 2019, le contrôlé ne remet pas en cause les constatations faites par le chef d'enquête et indique qu'à la suite du manquement constaté, une adresse e-mail dédiée a été créée « *afin que les personnes concernées puissent contacter directement le Délégué à la protection des données (« DPD »).* » Le contrôlé précise ensuite où les coordonnées du DPD ont été publiées, à savoir sur son site internet ainsi que dans sa politique en matière de traitement des données personnelles.

19. Lors de la séance du 31 mai 2021, la formation restreinte a relevé que les coordonnées du DPD n'étaient pas mentionnées dans la section du site internet du contrôlé relative à l'exercice des droits des personnes concernées ni dans le formulaire se trouvant sous cette section et a demandé au contrôlé un complément d'information à cet égard. Par courriel du 4 juin 2021, le contrôlé a informé la formation restreinte de la mention des coordonnées du DPD dans cette section ainsi que dans ledit formulaire.

20. Si des mesures ont été prises par le contrôlé afin de se conformer à l'obligation de publication des coordonnées de son DPD, il convient de relever que celles-ci ont été décidées seulement en cours d'enquête. La formation restreinte retient, qu'au début de l'enquête, le contrôlé n'avait pas publié les coordonnées de son DPD.

21. 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 d'associer le DPD à toutes les questions relatives à la protection des données à caractère personnel

1. Sur les principes

22. 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.

23. 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* »[7].

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

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

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

- de consulter immédiatement le DPD lorsqu'une violation de données ou un autre incident se produit.

25. Selon les lignes directrices concernant les DPD, l'organisme pourrait, le cas échéant, élaborer des lignes directrices ou des programmes en matière de protection des données indiquant les cas dans lesquels le DPD doit être consulté.

2. <u>En l'espèce</u>

26. 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.

27. Selon la communication des griefs, page 3, « [i]*l ressort de l'enquête que le DPD intervient sur invitation ou de manière ad hoc aux différentes réunions internes ou comités auxquels sont discutées les problématiques ou les projets avec des impacts en matière de protection des données, mais il n'existe pas de règle ou de fréquence définie quant à la participation du DPD à ces comités. »* Le chef d'enquête relève ensuite que « [l]*e fait que le DPD ait participé à deux Comités de Contrôle Interne (janvier 2019 et août 2018), au Management Board de novembre 2017, qu'il soit invité permanent du Comité de Sécurité et qu'il soit impliqué si un aspect Data Protection concerne un nouveau produit ne suffit pas à démontrer le caractère formel, permanent et régulier de l'implication du DPD.* »

28. Dans sa prise de position du 15 novembre 2019, le contrôlé indique que le DPD est intervenu de façon ad hoc en septembre 2019 au « Comité de Contrôle interne » et au « Comité Exécutif ». Il indique ensuite qu'une « *intervention trimestrielle au Comité de Contrôle Interne sera mise en place et formalisée »* dans sa « *Politique de protection des données personnelles* »*.*

29. La formation restreinte relève qu'il est 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. »

30. Or, la formation restreinte constate qu'il est aussi précisé en page 2 de la communication des griefs que le contrôlé compte environ […] employés et […] clients. Le chef d'enquête en conclut que le contrôlé traite un nombre significatif de données personnelles. La formation restreinte partage cette appréciation et considère dès lors que la participation formalisée et systématique du DPD aux réunions pertinentes, telle qu'elle est attendue par le chef d'enquête, constitue une mesure proportionnée afin d'assurer l'association du DPD à toutes les questions relatives à la protection des données personnelles.

31. La formation restreinte prend note du fait que dans sa réponse du 8 septembre 2020 au courrier complémentaire à la communication des griefs, le contrôlé a fourni des « *éléments d'information complémentaires (…) afin de répondre aux mesures correctrices proposées par le chef d'enquête* », concernant notamment l'association du DPD à toutes les questions relatives à la protection des données. Le contrôlé y a fourni une liste de 6 comités (concernant les domaines de l'IT, de la gestion du risque et de la sous-traitance) dont le DPD est membre permanent ainsi que des indications sur les interventions/participations du DPD à d'autres comités et réunions (à savoir le Comité « *[…]* », les réunions « *[…]*» et le Comité de contrôle interne « *afin de présenter le rapport d'activité trimestriel ou tout autre sujet qu'il juge nécessaire* »).

32. Si ces mesures devraient faciliter l'association du DPD 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. La formation restreinte considère dès lors que, au début de l'enquête, le responsable de traitement n'a pas été en mesure de démontrer que le DPD était associé de manière appropriée à toutes les questions relatives à la protection des données personnelles.

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

C. <u>Sur le manquement à l'obligation de garantir l'autonomie du DPD</u>

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

34. Aux termes de l'article 38.3 du RGPD, l'organisme doit veiller à ce que le DPD « ne reçoive aucune instruction en ce qui concerne l'exercice des missions ». Par ailleurs, le DPD « fait directement rapport au niveau le plus élevé de la direction » de l'organisme.

35. Le considérant (97) du RGPD indique en outre que les DPD « devraient être en mesure d'exercer leurs fonctions et missions en toute indépendance ».

36. Selon les lignes directrices concernant les DPD[8], l'article 38.3 du RGPD « *prévoit certaines garanties de base destinées à faire en sorte que les DPD soient en mesure d'exercer leurs missions avec un degré suffisant d'autonomie au sein de leur organisme. […] Cela signifie que, dans l'exercice de leurs missions au titre de l'article 39, les DPD ne doivent pas recevoir d'instructions sur la façon de traiter une affaire, par exemple, quel résultat devrait être obtenu, comment enquêter sur une plainte ou s'il y a lieu de consulter l'autorité de contrôle. En outre, ils ne peuvent être tenus d'adopter un certain point de vue sur une question liée à la législation en matière de protection des données, par exemple, une interprétation particulière du droit. […] Si le responsable du traitement ou le sous-traitant prend des décisions qui sont incompatibles avec le RGPD et l'avis du DPD, ce dernier devrait avoir la possibilité d'indiquer clairement son avis divergent au niveau le plus élevé de la direction et aux décideurs. À cet égard, l'article 38, paragraphe 3, dispose que le DPD « fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant ». Une telle reddition de compte directe garantit que l'encadrement supérieur (par ex., le conseil d'administration) a connaissance des avis et recommandations du DPD qui s'inscrivent dans le cadre de la mission de ce dernier consistant à informer et à conseiller le responsable du traitement ou le sous-traitant. L'élaboration d'un rapport annuel sur les activités du DPD destiné au niveau le plus élevé de la direction constitue un autre exemple de reddition de compte directe.* »

2. <u>En l'espèce</u>

37. Il ressort du rapport d'audit que, pour que le chef d'enquête considère l'objectif 7 comme rempli par le contrôlé dans le cadre de cette campagne d'audit, il s'attend à ce que le DPD soit « *rattaché au plus haut niveau de la direction afin de garantir au maximum son autonomie* ».

[8] WP 243 v.01, version révisée et adoptée le 5 avril 2017, p. 17 et 18

38. D'après la communication des griefs, page 4, « *Lors de l'enquête, les agents de la CNPD ont constaté l'existence de plusieurs intermédiaires hiérarchiques entre le DPD et la Direction. En effet, le DPD est rattaché à une personne du département « […] » qui est elle-même rattachée à une personne du département « […] » qui est elle-même rattachée au Chief Compliance Officer. Bien que le DPD puisse intervenir de manière ad hoc au Comité exécutif et au Comité de contrôle interne à sa demande et à tout moment, le rattachement hiérarchique à la Direction et donc l'accès à cette dernière ne sont pas directs et permanents.* »

39. Dans son courrier du 8 septembre 2020, le contrôlé indique qu'afin de garantir l'autonomie du DPD : « *i. la fonction de DPD a été rattachée hiérarchiquement au Chief Compliance Officer (CCO) du Groupe A compter du 15 janvier 2020. ii. Le CCO est invité permanent du Comité Exécutif de la Société A depuis le 1er octobre 2018 (pas d'intermédiaire hiérarchique entre le DPD et le plus haut niveau de la Direction) et rapporte directement au Chief Executive Officer, ainsi qu'au Président du Conseil d'administration. iii. Un rapport d'activité trimestriel sur la protection des données est présenté par le DPD à […] composé d'une partie du Comité Exécutif).* » Le contrôlé indique en outre que des réunions hebdomadaires sont organisées entre le DPD et le CCO.

40. S'il ne résulte pas des dispositions du RGPD que le DPD doit nécessairement être rattaché au niveau le plus élevé de la direction afin de garantir son autonomie, la formation restreinte rappelle néanmoins qu'elle a relevé au point 29 de la présente décision qu'il est 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.* »

41. Or, tel que cela est mentionné au point 30 de la présente décision, la formation restreinte partage l'appréciation du chef d'enquête, mentionnée en page 2 de la communication des griefs, selon laquelle le contrôlé traite un nombre significatif de données personnelles. La formation restreinte considère dès lors que, en l'absence d'autres mesures qui permettraient de démontrer que la reddition de compte directe auprès du plus haut niveau de la direction est formalisée, le rattachement hiérarchique du DPD au plus haut niveau de la direction, suivant l'attente du chef d'enquête, constitue une mesure proportionnée afin de garantir son autonomie.

42. A cet égard, la formation restreinte constate qu'au moment de l'ouverture de l'enquête, le DPD n'était pas rattaché au plus haut niveau de la direction et qu'il n'a pas été démontré par le contrôlé que la reddition de compte directe auprès du plus haut niveau de la direction était formalisée.

43. Au vu de ce qui précède, la formation restreinte conclut que l'article 38.3 du RGPD n'a pas été respecté par le contrôlé.

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

1. Sur les principes

44. 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 États 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.

45. Il résulte des lignes directrices concernant les DPD[9] que le DPD peut, dans le cadre de ces 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. En l'espèce

46. 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)* ».

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

47. Selon la communication des griefs, p. 5, *«* [i] *l ressort de l'enquête que l'organisme ne dispose pas de plan de contrôle. Bien que l'organisme a informé la CNPD que des contrôles relatifs à la protection des données sont en cours de construction, qu'ils seront intégrés dans le Compliance Monitoring program et que le recours à de l'assistance externe est envisagée pour construire ce programme de monitoring, l'organisme n'effectuait pas les missions de contrôle au moment de l'enquête.* »

48. Dans son courrier du 8 septembre 2020, le contrôlé indique avoir « *demandé l'aide de consultants pour l'élaboration d'un plan de contrôle […] »* et que *« [c]e [plan] a été finalisé en* [d]*écembre 2019 et est applicable en 2020 ».* Le contrôlé indique en outre qu'en *« avril 2019 l'Audit Interne* [du contrôlé] *(3ème ligne de défense) a mené une mission sur l'implémentation du règlement (UE) 2016/679 ayant donné lieu à des recommandations.* » Le contrôlé précise aussi que *« des contrôles ont été réalisés ou sont en cours de réalisation par le DPD* », notamment la revue du registre des traitements et la revue des clauses contractuelles relatives à la protection des données. Le contrôlé indique enfin que « *conformément à l'article 25 du règlement, les principes de « protection des données dès la conception et protection des données par défaut » ont été mis en place comme contrôle a priori pour la mise en place de nouveaux traitements de données personnelles.* »

49. 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 « *[c]e 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 ou du sous-traitant*.[10] »

50. Il ressort des réponses du contrôlé au questionnaire préliminaire que, dès le début de l'enquête, le DPD avait pour tâche de « *coordonner la documentation des traitements dans le registre* »[11]. La formation restreinte relève néanmoins que cet élément pris isolément ne suffit pas à démontrer que la mission de contrôle du respect du RGPD ait pu être effectuée de manière adéquate.

[10] WP 243 v.01, version révisée et adoptée le 5 avril 2017, p. 22
[11] Réponse du contrôlé du 28/09/2018 au questionnaire préliminaire (question 5.d).

51. La formation restreinte rappelle qu'elle a relevé au point 29 de la présente décision qu'il est 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.* »

52. Or, tel que cela est mentionné au point 30 de la présente décision, la formation restreinte partage l'appréciation du chef d'enquête, mentionnée en page 2 de la communication des griefs, selon laquelle le contrôlé traite un nombre significatif de données personnelles.

53. La formation restreinte considère par conséquent que la mission de contrôle effectuée par le DPD auprès du contrôlé devrait être suffisamment 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 manière adéquate.

54. La formation restreinte prend note des éléments communiqués par le contrôlé dans son courrier du 8 septembre 2020 concernant l'élaboration d'un plan de contrôle finalisé en décembre 2019 et son application en 2020.

55. Néanmoins, la formation restreinte constate que ce plan de contrôle a été établi après le début de l'enquête et considère dès lors qu'au début de l'enquête, le contrôlé n'a pas été en mesure de démontrer que le DPD exerce ses missions de contrôle du respect du RGPD de manière adaptée à ses besoins.

56. 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 l'amende

A. Les principes

57. 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.* »

58. 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 ».

59. 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.

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

B. En l'espèce

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

61. Dans son courrier complémentaire à la communication des griefs du 3 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 18.700 euros.

62. 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, 38.3, 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 afin de pouvoir prendre contact avec le DPD au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice de leurs droits, où le DPD est associé dès le stade le plus précoce possible à toutes les questions relatives à la protection des données, puisse exercer ses fonctions et missions en toute indépendance, et puisse exercer de façon effective ses missions, notamment la mission de contrôle du respect du RGPD.

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

(1) Que le contrôlé a indiqué dans sa prise de position du 15 novembre 2019 qu'une adresse e-mail dédiée a été créée « afin que les personnes concernées puissent contacter directement le Délégué à la protection des données » et que les coordonnées du DPD ont été publiées sur son site internet ainsi que dans sa politique en matière de traitement des données personnelles. 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 novembre 2019.

(2) Qu'il a été décidé par le contrôlé de prendre des mesures adaptées afin de faciliter l'association du DPD à toutes les questions relatives à la protection des données, lesquelles sont décrites dans son courrier du 8 septembre 2020. Le manquement à l'article 38.1 du RGPD a donc duré dans le temps, à tout le moins entre le 25 mai 2018 et septembre 2020 ;

(3) Que les éléments communiqués par le contrôlé en cours d'enquête, et notamment par courriel du 4 juin 2021 suite à la séance du 31 mai 2021, ne permettent pas de démontrer que le DPD serait en mesure de rendre compte directement au plus haut niveau de la direction de manière formalisée. Le manquement à l'article 38.3 du RGPD a donc duré dans le temps, à compter du 25 mai 2018, étant précisé que la formation restreinte n'a pas pu constater que le manquement a pris fin ;

(4) Qu'un plan de contrôle a été finalisé en décembre 2019 et appliqué en 2020. Le manquement à l'article 39.1.b) du RGPD a donc duré dans le temps, à tout le moins entre le 25 mai 2018 et décembre 2019.

63. 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.

64. La formation restreinte relève que si plusieurs mesures ont été décidées par le contrôlé afin de remédier aux 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 (voir aussi le point 59 de la présente décision).

65. 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, 38.1, 38.3 et 39.1.b) du RGPD.

66. 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, 38.3, 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.

67. 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 18.700 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

68. Dans son courrier complémentaire à la communication des griefs du 3 août 2020, le chef d'enquête propose à la formation restreinte de prendre les mesures correctrices suivantes :

> « *a) Ordonner la publication des coordonnées du délégué à la protection des données conformément aux exigences de l'article 37 paragraphe 7 du RGPD et aux lignes directrices relatives au DPD du groupe de travail " article 29 " sur la protection des données qui indiquent que les personnes concernées doivent pouvoir aisément et directement prendre contact avec le DPD sans devoir s'adresser à un autre service de l'organisme. Ainsi, une des manières pour parvenir à ce résultat serait de publier les coordonnées du DPD sur le site web public de la [Société A] dans la mesure où ce ne serait pas déjà fait.*
>
> *b) Ordonner la mise en place de mesures assurant une association du DPD à toutes les questions relatives à la protection des données, conformément aux exigences de l'article 38 paragraphe 1 du RGPD. Bien que plusieurs manières puissent être envisagées pour parvenir à ce résultat, une des possibilités pourrait être 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 avec l'agenda des réunions, invitation, fréquence, statut de membre permanent, etc....).*

c) Ordonner la mise en place d'un mécanisme garantissant l'autonomie du DPD conformément aux exigences de l'article 38 paragraphe 3 du RGPD. Plusieurs mesures peuvent être envisagées pour parvenir à ce résultat, telles que le rattachement du DPD au plus haut niveau de la direction afin de garantir au maximum son autonomie ou la création d'une ligne formalisée et régulière de reporting direct, ainsi qu'un mécanisme d'escalade d'urgence à la direction permettant de contourner le(s) niveau(x) hiérarchique(s) intermédiaire(s).

d) Ordonner le déploiement de la mission de contrôle, conformément à l'article 39 paragraphe 1 b) du RGPD. Le DPD devrait ainsi documenter ses contrôles relatifs à 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 dans la mesure où ce ne serait pas déjà fait.»

69. Quant aux mesures correctrices proposées par le chef d'enquête et par référence au point 60 de la présente décision, la formation restreinte prend en compte les démarches effectuées par le contrôlé afin de se conformer aux dispositions des articles 37.7, 38.1, 38.3, et 39.1.b) du RGPD, notamment les mesures décrites dans son courrier du 15 novembre 2019 et dans son courrier du 8 septembre 2020. Plus particulièrement, elle prend note des faits suivants :

- En ce qui concerne la violation de l'article 37.7 du RGPD, la formation restreinte constate qu'une adresse e-mail dédiée a été créée et que les coordonnées du DPD ont été publiées sur le site internet du contrôlé ainsi que dans sa politique en matière de traitement des données personnelles. La formation restreinte considère dès lors qu'il n'y a pas lieu de prononcer la mesure correctrice proposée par le chef d'enquête sous a) du point 68 de la présente décision.

- En ce qui concerne la violation de l'article 38.1 du RGPD, la formation restreinte constate qu'il a été décidé par le contrôlé de prendre des mesures adaptées afin de faciliter l'association du DPD à toutes les questions relatives à la protection des données. La formation restreinte considère dès lors qu'il n'y a pas lieu de prononcer la mesure correctrice proposée par le chef d'enquête sous b) du point 68 de la présente décision.

- En ce qui concerne la violation de l'article 38.3 du RGPD, la formation restreinte constate que les éléments communiqués par le contrôlé en cours d'enquête, et notamment par courriel du 4 juin 2021 suite à la séance du 31 mai 2021, ne permettent pas de démontrer

que le DPD serait en mesure de rendre compte directement au plus haut niveau de la direction de manière formalisée. La formation restreinte considère dès lors qu'il y a lieu de prononcer la mesure correctrice proposée par le chef d'enquête sous c) du point 68 de la présente décision.

- En ce qui concerne la violation de l'article 39.1.b) du RGPD, la formation restreinte relève qu'un plan de contrôle a été finalisé en décembre 2019 et appliqué en 2020. La formation restreinte considère dès lors qu'il n'y a pas lieu de prononcer la mesure correctrice proposée par le chef d'enquête sous d) du point 68 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, 38.3 et 39.1.b) du RGPD ;

- de prononcer à l'encontre de la Société A une amende administrative d'un montant de dix-huit mille sept cent euros (18.700 euros) au regard de la violation des articles 37.7, 38.1, 38.3 et 39.1.b) du RGPD ;

- de prononcer à l'encontre de la Société A une injonction de se mettre en conformité avec l'article 38.3 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 en place et du maintien d'un mécanisme formel garantissant l'autonomie du DPD.

Ainsi décidé à Belvaux en date du 27 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.