

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

Délibération n° 5FR/2023 du 5 juillet 2023

La Commission nationale pour la protection des données siégeant en formation restreinte, composée de Madame Tine A. Larsen, présidente, et de Messieurs Thierry Lallemand et Marc Lemmer, commissaires ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE ;

Vu la loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, notamment son article 41 ;

Vu le règlement d'ordre intérieur de la Commission nationale pour la protection des données adopté par décision n°3AD/2020 en date du 22 janvier 2020, notamment son article 10.2 ;

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

Considérant ce qui suit :

I. Faits et procédure

1. En date du 10 mars 2021, la Commission nationale pour la protection des données (ci-après : la « CNPD » ou la « Commission nationale ») a été saisie d'une réclamation de Madame [...] (ci-après : « la réclamante ») concernant la publication de ses [données] [sur le site internet] de la Société X (ci-après : « Société X ») et signalant à la CNPD de potentielles violations des dispositions 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 (ci-après : le « RGPD »).
2. Dans le cadre de l'instruction de la réclamation, il est apparu que la Société A [...] avait transféré les données à caractère personnel de la réclamante à la Société B qui elle-même a transféré lesdites données à la Société X. Lors de sa séance de délibération du 1^{er} juillet 2022, la Commission nationale pour la protection des données siégeant en formation plénière a dès lors décidé d'ouvrir une enquête auprès des sociétés A, B et C sur base de l'article 38 de la loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données (ci-après : « loi du 1^{er} août 2018 ») et de désigner Monsieur Alain Herrmann comme chef d'enquête.
3. Ladite décision a précisé que l'enquête menée par la CNPD avait pour objet de contrôler l'application et le respect par les trois sociétés susmentionnées « *des dispositions du RGPD, notamment celles relatives à la base de licéité du traitement, à l'obligation d'information de la personne concernée quant au transfert de ses données à des tiers et au droit à l'effacement, dans le cadre particulier du transfert des données à caractère personnel de la réclamante à une société tierce.* »
4. La Société A est inscrite au registre du Commerce et des Sociétés de Luxembourg sous le numéro [...] et a son siège social au [...], [...] (ci-après : le « contrôlé »). Il [offre des services de communications électroniques].¹

¹ Voir article [...] de sa constitution de société du [...] déposé le [...].

5. La décision de la Commission nationale siégeant en formation restreinte (ci-après: la « Formation Restreinte ») sur l'issue de l'enquête se basera :
- sur les traitements effectués par le contrôlé dans le cadre de la réclamation susmentionnée et contrôlés par les agents de la CNPD ; et
 - sur les dispositions légales et réglementaires prises en compte par le chef d'enquête dans sa communication des griefs.
6. Le contrôlé a été informé de l'ouverture de l'enquête à son égard par courrier du chef d'enquête en date du 23 août 2022. Il ressort de ce courrier que le chef d'enquête avait défini les objectifs de contrôle suivants :
- « • Déterminer la qualification juridique des entités contrôlées au regard du RGPD afin de savoir quelle(s) entité(s) est/sont responsable(s) du traitement et/ou sous-traité(s) ;
- Vérifier la base de licéité du transfert des données à caractère personnel de la réclamante par la Société A vers la/les société(s) Société B et/ou Société C ;
 - Vérifier la base de licéité du transfert des données à caractère personnel de la réclamante par les entités visées vers la Société X ;
 - Vérifier le respect par le(s) responsable(s) du traitement de son obligation d'information de la personne concernée quant au transfert de données à caractère personnel vers une société tierce ;
 - Vérifier que le(s) responsable(s) du traitement a/ont fait droit à la demande d'effacement et/ou au droit d'opposition de la personne concernée. »
7. Le courrier était accompagné du document intitulé « Constats initiaux Enquête n°[...] » exposant les constats initiaux réalisés par les agents de la CNPD sur base des pièces collectées dans le cadre de la réclamation et versées à la présente enquête (ci-après : les « constats initiaux »). Le chef d'enquête a offert la faculté au contrôlé de « contester les faits repris dans les constats initiaux, ou faire part de [ses] éventuels remarques, précisions ou ajouts » pour le 7 octobre 2022 au plus tard.
8. Le contrôlé a répondu par courrier en date du 7 octobre 2022.
9. A l'issue de son instruction, le chef d'enquête a notifié au contrôlé en date du 25 janvier 2023 une communication des griefs détaillant les manquements qu'il estimait constitués en l'espèce par rapport aux exigences prescrites par l'article 13.1.e) du RGPD (obligation

d'information relative aux destinataires ou catégories de destinataires des données à caractère personnel) et par l'article 24.1 du RGPD (obligation de mettre en œuvre des mesures techniques et organisationnelles appropriées).

Le chef d'enquête a proposé à la Formation Restreinte d'adopter deux mesures correctrices différentes, ainsi que d'infliger au contrôlé une amende administrative d'un montant de 1.500 euros.

La faculté de formuler ses observations écrites sur la communication des griefs a été offerte au contrôlé. Ce dernier n'a pas communiqué d'observations au chef d'enquête.

10. La présidente de la Formation Restreinte a informé le contrôlé par courrier en date du 13 mars 2023 que son affaire serait inscrite à la séance de la Formation Restreinte du 27 avril 2023 et qu'il lui était offert la possibilité d'y être entendu. Par courriel du 18 avril 2023, le contrôlé a confirmé sa présence à ladite séance.

Lors de cette séance le chef d'enquête et le contrôlé, représenté par Monsieur [...], ont exposé leurs observations orales à l'appui de leurs observations écrites et ont répondu aux questions posées par la Formation Restreinte. Le contrôlé a eu la parole en dernier.

II. En droit

II.1. Sur la qualité du contrôlé à l'égard des traitements en cause

1. Sur les principes

12. Conformément à l'article 4 point 7) du RGPD, le responsable du traitement est « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement [...]* ».

11. L'article 4 point 8) du RGPD quant à lui définit le sous-traitant comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.* »

12. Le Comité Européen de la Protection des Données (ci-après le : « CEPD ») a fourni des explications supplémentaires dans ses lignes directrices sur les notions de responsable du traitement et de sous-traitant qui « *ont un rôle capital à jouer dans l'application du [RGPD], étant donné qu'elles déterminent qui est responsable du respect des différentes règles en matière de protection des données et la manière dont les personnes concernées peuvent*

exercer leurs droits dans la pratique. » Il y est précisé que lesdites notions sont des « notions fonctionnelles en ce qu'elles visent à répartir les responsabilités en fonction des rôles réels joués par les parties et des notions autonomes en ce qu'elles doivent être interprétées principalement selon la législation de l'UE en matière de protection des données. »²

2. En l'espèce

13. Par courrier du 7 octobre 2022 le contrôlé a expliqué [...] que la « *gestion et l'administration de la Société A sont assurées par la Société B et la Société C conformément au contrat de collaboration conclu entre actionnaires le [...] (Annexe 1). En effet, [...] toutes les tâches sont réparties entre la Société B et la Société C conformément à l'annexe du contrat de collaboration ci-avant mentionnée (annexe 2).* »

14. Dans le courrier précité du 7 octobre 2022, le contrôlé a par ailleurs expliqué qu' « *étant une société bénéficiant de clients en propre, [il] est responsable de traitement au regard de ces derniers. La Société B et la Société C ne sont pas responsables de traitement conjoints contrairement à ce qui vous a été indiqué par la salariée de la Société B et repris dans la pièce numéro 9 du dossier. La Société B et la Société C sont sous-traitants pour le compte de la Société A comme en attestent les contrats de sous-traitances conclus par la Société A avec ces deux sociétés (Annexe 3 et 4).* »

Il ressort du même courrier que son sous-traitant la Société B (ci-après : « la Société B » ou le « sous-traitant ») est chargé de transmettre pour son compte les fichiers clients à la Société X pour publication [sur son site internet].

15. Comme la réclamante a souscrit en date du 27 avril 2015³ un contrat d'abonnement avec le contrôlé, ce dernier est à considérer comme responsable du traitement des données à caractère personnel de la réclamante dans le cadre dudit contrat, tandis que la Société B agit dans ce contexte spécifique comme sous-traitant du contrôlé en ayant pour mission de gérer [les fichiers clients] conformément au contrat de sous-traitance précité.

16. Lors de la séance de la Formation Restreinte du 27 avril 2023, le contrôlé a confirmé les qualités précitées de la Société A et de la Société B, tout en précisant que les deux entités n'ont pas de fichier clients commun et que chacune a son propre système informatique. Néanmoins, en vertu du contrat de sous-traitance, du personnel du sous-traitant aurait

² CEPD, Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, Version 2.0, Adoptées le 7 juillet 2021, page 3.

³ Voir pièce 2 annexée à la communication des griefs.

accès au système informatique du contrôlé pour faire les opérations nécessaires pour son compte, [...], d'une part, et d'envoyer ledit fichier mensuellement à la Société X (sauf s'il n'y a pas eu de modification par rapport au mois précédent), d'autre part.

II. 2. Sur les motifs de la décision

A. Sur le manquement lié à l'obligation d'informer les personnes concernées

1. Sur les principes

17. Aux termes de l'article 12.1 du RGPD, le « *responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant. Les informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique. Lorsque la personne concernée en fait la demande, les informations peuvent être fournies oralement, à condition que l'identité de la personne concernée soit démontrée par d'autres moyens.* »

18. L'article 13 du RGPD prévoit ce qui suit :

« 1. Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement lui fournit, au moment où les données en question sont obtenues, toutes les informations suivantes :

[...]

e) les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent ;

[...]

19. Conformément à l'article 4 point 9) du RGPD on entend par « *destinataire* », la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. [...] ».

20. La transparence constitue un aspect fondamental des principes relatifs au traitement des données à caractère personnel.⁴ Les obligations en la matière ont été explicitées par le Groupe de Travail Article 29 dans ses lignes directrices sur la transparence au sens du règlement (UE) 2016/679, dont la version révisée a été adoptée le 11 avril 2018 (ci-après : « WP 260 rév.01 » ou les « lignes directrices sur la transparence »).

Ces lignes directrices explicitent en particulier les règles générales de transparence établies par l'article 12 du RGPD, et qui sont applicables à la communication d'informations aux personnes concernées (Articles 13 et 14 du RGPD), aux communications adressées aux personnes concernées au sujet de l'exercice de leurs droits (Articles 15 à 22 du RGPD), et aux communications concernant les violations de données (Article 34 du RGPD).⁵

21. A noter que le CEPD, qui a succédé au Groupe de Travail Article 29 le 25 mai 2018, a repris et réapprouvé les documents adoptés par ledit Groupe entre le 25 mai 2016 et le 25 mai 2018, comme précisément les lignes directrices précitées sur la transparence.⁶

2. En l'espèce

22. Par courrier du 7 octobre 2022, le contrôlé a transmis au chef d'enquête les « *conditions générales de la Société A actuellement en vigueur. Vous pouvez constater que ces dernières font bien état des traitements de données réalisés par la Société B et la Société C dans le cadre de la sous-traitance (annexe 5).* »

23. Dans un courrier du 11 novembre 2022, le chef d'enquête a néanmoins estimé que ces conditions générales n'ont été créés que « *récemment puisque, d'une part, le lien url permettant d'y accéder contient la date du [...] 2022 et, d'autre part, les métadonnées du document « pdf » mentionnent comme date de création [...] octobre 2022 (voir annexe).* »

Il a dès lors demandé dans ledit courrier au contrôlé d'indiquer « *si un tel document d'information était disponible sur le site [...] à la date de la signature du contrat d'abonnement de la Société A de Madame [...] [le 27 avril 2015]. En cas de réponse positive, merci de nous transmettre la version de ce document d'information tel que disponible sur le site [...] à cette même date.* »

⁴ Voir notamment les articles 5.1.a) et 12 du RGPD, voir aussi les considérants (39), (58) à (60) du RGPD.

⁵ WP 260 rév.01, point 7.

⁶ Voir décision Endorsement 1/2018 du CEPD du 25 mai 2018, disponible sous : https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

24. Par courrier du 28 novembre 2022, le contrôlé a envoyé le contrat de la réclamante signé en date du 27 avril 2015 ensemble avec un formulaire d'acceptation des conditions générales alors en vigueur. Il a néanmoins indiqué qu'à la date de signature des contrats, les conditions générales signées par les clients n'auraient pas été systématiquement conservées et il a donc envoyé les conditions générales signées par un autre client en date du 14 septembre 2014, tout en précisant que les conditions générales n'auraient pas évoluées entre cette date et la date de signature du contrat de la réclamante.
25. Dans la communication des griefs du 25 janvier 2023, le chef d'enquête a dès lors acté que « [d]'après le contrôlé, la Réclamante a signé, en même temps que son contrat d'abonnement, les conditions générales des services de la Société A alors en vigueur (PIECE 2) ». ⁷
26. Il a par ailleurs noté que le contrôlé a conclu avec son sous-traitant la Société B un contrat de sous-traitance le [...] 2017, qui a fait l'objet d'un avenant en date du [...] 2018 et qui prévoit un transfert des données des abonnés du contrôlé audit sous-traitant. Il en a conclu que « [l]information selon laquelle la Société B est destinataire des données à caractère personnel des abonnés de la Société A devrait donc figurer dans les informations transmises par le Contrôlé aux personnes concernées depuis la signature dudit contrat de sous-traitance, conformément à l'article 26, paragraphe 1, lettre (c) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, puis conformément au RGPD à compter du 25 mai 2018. »⁸
27. Par ailleurs, le chef d'enquête a noté que « les conditions générales des services de la Société A, mises à disposition des personnes concernées sur le site internet [...], n'ont pas été mises à jour suite à la signature par le Contrôlé du contrat de sous-traitance avec la Société B, ni suite à l'entrée en application du RGPD.

En effet, comme le montre la capture d'écran [...], les conditions générales de la Société A disponibles sur le site internet [...] sont les mêmes entre [...] 2014 et [...] 2022 (PIECE 4).

En outre, le Contrôlé a transmis aux agents de la CNPD en charge de l'enquête les conditions générales de la Société A telles que disponibles sur le site internet [...] en date du [...] octobre 2022 (PIECE 5). Ces conditions générales précisent effectivement que les

⁷ Communication des griefs, point 21.

⁸ Communications des griefs, points 22 à 23.

données à caractère personnel des abonnés de la Société A sont transférées à la Société B.

Cependant, ces conditions générales ont été mises à disposition des personnes concernées sur le site internet [...] le [...] octobre 2022, comme le montre la capture d'écran des métadonnées du site internet [...] (PIECE 6), soit après l'ouverture de la présente enquête. »⁹

28. Ainsi, le chef d'enquête a retenu que « *les conditions de l'article 13, paragraphe 1, lettre e) du RGPD n'ont pas été respectées, le Contrôlé n'ayant pas mis à jour les informations mises à la disposition de la Réclamante relatives aux destinataires de ses données à caractère personnel, via son site internet [...] ou via un quelconque autre moyen.* »¹⁰

29. La Formation Restreinte rappelle que, même si le droit à l'information de la personne concernée était déjà ancré dans la loi abrogée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel,¹¹ au moins depuis le 25 mai 2018¹² le contrôlé aurait dû informer la réclamante, entre autres, sur les destinataires ou catégories de destinataires des données à caractère personnel.

30. Elle note tout d'abord que la réclamante a conclu un contrat d'abonnement avec le contrôlé en date du 27 avril 2015, c'est-à-dire avant l'entrée en application du RGPD, et qui a pris fin après l'entrée en application du RGPD, plus précisément en date du 30 juin 2019.

31. De même, la Formation Restreinte constate que les conditions générales que la réclamante a, d'après le contrôlé, signé en date du 25 avril 2015 en même temps que son contrat d'abonnement ne mentionnent aucun transfert de données vers un sous-traitant¹³, tandis que les conditions générales transmises par le contrôlé au chef d'enquête en date du [...] octobre 2022 contiennent un point spécifique sur la sous-traitance dans la partie plus globale concernant le traitement de données.¹⁴

⁹ Communication des griefs, point 24.

¹⁰ Communication des griefs, point 25.

¹¹ Cette loi, qui a été abrogée par la loi du 1er août 2018, prévoyait dans son article 26.1 c), premier tiret le droit à l'information de la personne concernée sur « *les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées.* »

¹² Date de l'entrée en application du RGPD.

¹³ Voir annexe 3 du courrier du contrôlé du 28 novembre 2022.

¹⁴ Voir la partie [...].

32. Elle constate de même que d'après le chef d'enquête, ces dernières conditions générales n'ont été mises à disposition des clients qu'en date du [...] octobre 2022.¹⁵
33. Lors de la séance de la Formation Restreinte du 27 avril 2023, le contrôlé a indiqué que des mises à jour des conditions générales auraient été réalisées fréquemment, mais qu'il n'aurait pas gardé l'historique des différentes versions. Il a par ailleurs contesté formellement que cette mention de la sous-traitance n'aurait été insérée qu'en 2022, tout en avouant qu'il ne dispose pas de version des conditions générales existantes entre 2015 et 2022 et qu'il a dès lors aucune preuve quand cette mise à jour intégrant la sous-traitance a réellement eu lieu.
34. Ainsi, la Formation Restreinte constate qu'elle n'a obtenu aucune documentation contenant une preuve attestant que le contrôlé a mis à jour ses conditions générales après l'entrée en application du RGPD et avant octobre 2022. Elle doit en conclure qu'elle ne dispose d'aucune preuve que la réclamante a eu des informations par le contrôlé relatives aux destinataires de ses données à caractère personnel, via son site internet [...] ou via un quelconque autre moyen, après l'entrée en application du RGPD et jusqu'à la résiliation de son contrat d'abonnement en juin 2019, voire jusqu'à la dernière transmission de ses données à caractère personnel à la Société B en février 2022.
- Par ailleurs, elle ne dispose pas non plus de preuves que les autres clients du contrôlé ont été informé sur les destinataires de leurs données à caractère personnel, et plus précisément sur le transfert de leurs données au sous-traitant [...], après l'entrée en application du RGPD et jusqu'en octobre 2022.
35. Au vu de ce qui précède, la Formation Restreinte se rallie au chef d'enquête et conclut qu'au début de l'enquête¹⁶, le contrôlé a manqué à son obligation découlant de l'article 13.1. e) du RGPD.
36. Quant aux mesures prises par le contrôlé après le début de l'enquête, la Formation Restreinte y revient au point 62, ainsi qu'au Chapitre II.3. Section 2.2. de cette décision.

¹⁵ Voir communication des griefs, point 24 et point 27 de la présente décision.

¹⁶ C'est-à-dire au moment de la réception du courrier du chef d'enquête informant le contrôlé de l'ouverture de l'enquête à son égard en date du 23 août 2022.

B. Sur le manquement lié à l'obligation de mettre en œuvre des mesures techniques et organisationnelles appropriées conformément à l'article 24 du RGPD

1. Sur les principes

37. Aux termes de l'article 5.2 du RGPD, le « *responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité).* »

38. L'article 24 du RGPD, intitulé « Responsabilité du responsable du traitement » quant à lui prévoit en son paragraphe premier que « *[c]ompte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire.* »

2. En l'espèce

39. Le contrat d'abonnement conclu le 27 avril 2015 entre le contrôlé et la réclamante a pris fin en date du 30 juin 2019.

40. Néanmoins, il ressort des constats initiaux qu'en octobre 2020, suite à un appel de prospection téléphonique à des fins religieuses, la réclamante s'est rendue compte que ses [données] étaient publiées [...] sur le site internet de la Société X et que lesdites [données] ont été transférées par la Société B pour le compte du contrôlé à la Société X pour publication [sur son site]. En date du 19 octobre 2020, la Société X a confirmé à la réclamante que ses données seraient supprimées de son site internet.

41. Or, le 10 mars 2021, les [données] de la réclamante étaient de nouveau disponibles sur le site internet de la Société X, cette dernière affirmant que lesdites [données] lui avaient encore une fois été transférées par la Société B pour publication [sur son site].

42. Par courrier du 1^{er} juin 2021, le sous-traitant [...] a précisé que la Société X a pris contact avec ses services en date du 29 mars 2021 afin de l'informer de la volonté de la réclamante de ne plus apparaître [sur son site], d'une part, et comme la réclamante n'était plus abonnée auprès du contrôlé depuis le 30 juin 2019, « *ses [données] n'auraient dès lors pas dû être transférées à la Société X [en] 2021. Ce transfert résulte d'une erreur de paramétrage interne et des mesures rectificatives ont été prises pour y remédier.* »

43. Or, suite à un autre appel de prospection téléphonique à des fins religieuses adressé à la réclamante en date du 5 mars 2022, il est apparu que ses [données] avaient de nouveau été publiées [sur le site] de la Société X, cette dernière affirmant que cette publication a eu lieu suite à un transfert desdites [données] par la Société B à la Société X en février 2022.
44. Par courrier du 7 octobre 2022, le contrôlé a reconnu « *un dysfonctionnement causé par une erreur humaine dans la transmission de fichier à la Société X par l'un de nos sous-traitants, en l'occurrence la Société B. En effet, les données concernant Madame [...] n'auraient pas dû être transmises à la Société X alors que son contrat avait été résilié. Nous reconnaissons également un délai de traitement anormalement long de la demande de la Société X visant à supprimer des listes Madame [...]. En tant que Responsable de traitement, nous comprenons que ces fautes sont imputables à la Société A. En effet, la Société A aurait dû s'assurer de la licéité du transfert de données à la Société X par ses sous-traitants.* »
45. Dans le même courrier, le contrôlé a par ailleurs formellement contesté d'avoir à nouveau transféré les données de la réclamante à la Société X en février 2022 et a insisté que selon « *les informations en notre possession, les données de Madame [...] ont été supprimées des listes transmises à la Société X le [29 mars 2022]¹⁷ et n'ont plus été transmises à la Société X par la suite.* »
46. Dans la communication des griefs du 25 janvier 2023, le chef d'enquête a acté que la Société X a reçu de la Société B les données de la réclamante afin de les faire figurer [sur son site] en 2020 et 2021, alors que « *[l]'abonnement de la Société A de la Réclamante a pris fin le 30 juin 2019, date à partir de laquelle la Société B, en tant que sous-traitante du Contrôlé, aurait dû cesser de transférer les données à caractère personnel de la Réclamante à la Société X*». ¹⁸
47. Par ailleurs, il a noté que les données à caractère personnel de la réclamante figuraient de nouveau dans le fichier contenant les données des abonnés de la Société A tel que transmis en février 2022 à la Société X, même si la Société B a assuré dans son courrier du 7 octobre 2022 que les données de la réclamante n'avaient plus été transmises à la Société X depuis le 29 mars 2021. De même, il était d'avis qu'une « *simple action de recherche « Ctrl+f » dans le fichier [...] tel que transmis par la Société B à la Société X le 23 mars 2022 permet pourtant de voir que les données de la Réclamante sont bien*

¹⁷ La Formation Restreinte suppose qu'il s'agit du 29 mars 2021.

¹⁸ Communication des griefs, point 28.

*présentes parmi les données des abonnés de la Société A à faire figurer [sur le site] de la Société X ».*¹⁹

48. Ainsi, le chef d'enquête a retenu qu'en « *tant que responsable du traitement, le Contrôlé n'a pas démontré la mise en œuvre de quelconques mesures techniques et organisationnelles lui permettant de vérifier le respect des dispositions du RGPD par son sous-traitant. En effet, le Contrôlé ne procède à aucun contrôle régulier de son sous-traitant et a répondu aux Constats Initiaux de la présente enquête sans prendre la peine de faire une simple vérification « Ctrl+f » dans les fichiers [...] de la Société B..* » Pour ces raisons, il était d'avis « *que les conditions de l'article 24, paragraphe 1, du RGPD n'ont pas été respectées, le Contrôlé n'ayant pas mis en œuvre des mesures techniques et organisationnelles appropriées de manière à ce que le traitement des données de la Réclamante réponde aux exigences du RGPD et garantisse la protection des droits de la personne concernée.* »²⁰

49. La Formation Restreinte tient à rappeler que l'article 24.1 du RGPD oblige chaque responsable du traitement de prendre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au RGPD. Cet article reflète le principe de « responsabilité » (« accountability » en anglais) énoncé à l'article 5.2 du RGPD, selon lequel « *le responsable du traitement est responsable du respect du paragraphe 1 (responsabilité) et est en mesure d'en apporter la preuve* ».

Par ailleurs, d'après le considérant (74) du RGPD, il « *y a lieu d'instaurer la responsabilité du responsable du traitement pour tout traitement de données à caractère personnel qu'il effectue lui-même ou qui est réalisé pour son compte. [...]* », c'est à dire effectué par un de ses sous-traitants.

50. Elle note dans ce contexte que depuis le 30 juin 2019, date de résiliation par la réclamante du contrat d'abonnement conclu avec le contrôlé, la réclamante n'aurait plus dû figurer sur la liste des abonnés souhaitant apparaître [sur le site internet] que la Société B transmet en principe mensuellement pour le compte du contrôlé à la Société X. Or, le sous-traitant a transmis les [données] de la réclamante précisément aux fins de publication [sur son site] en 2020, en 2021, ainsi qu'en février 2022. En effet, la Société B a fait parvenir en date du 14 décembre 2022, entre autres, le courriel et le fichier [...] envoyés le 15 février

¹⁹ Communication des griefs, point 32.

²⁰ Communication des griefs, points 33 et 34.

2022 à la Société X contenant les [données] des abonnés de la Société A souhaitant apparaître [sur le site] de la Société X, y inclus toujours celles de la réclamante.

51. Elle prend aussi en compte le courrier du 7 octobre 2022, dans lequel le contrôlé a reconnu « *un dysfonctionnement causé par une erreur humaine dans la transmission de fichier à la Société X par l'un de nos sous-traitants, en l'occurrence la Société B. En effet, les données concernant Madame [...] n'auraient pas dû être transmises à la Société X alors que son contrat avait été résilié. [...]. En tant que Responsable de traitement, nous comprenons que ces fautes sont imputables à la Société A. En effet, la Société A aurait dû s'assurer de la licéité du transfert de données à la Société X par ses sous-traitants.* »
52. Lors de la séance de la Formation Restreinte du 27 avril 2023, le contrôlé a par ailleurs confirmé que, contrairement aux affirmations précédentes, dans le fichier transmis en février 2022 à la Société X les [données] de la requérante y figuraient en effet encore. Il a expliqué que ces transmissions irrégulières étaient liées à un problème informatique interne, car au moment où l'abonnement de la réclamante avec la Société A a été résilié en 2019, l'inscription dans le fichier des personnes souhaitant apparaître [sur le site internet] de la Société X n'a pas été supprimée automatiquement. D'après le contrôlé, cette mise à jour dans le système informatique de la Société A [...] n'aurait été faite qu'en mars 2022.
53. Indépendamment des raisons qui ont menées à ces transmissions irrégulières des [données] de la réclamante à la Société X par le sous-traitant du contrôlé en 2020, en 2021, ainsi qu'en février 2022, la Formation Restreinte constate que les demandes de suppression des données de la réclamante par la Société X en date du 19 octobre 2020 et du 29 mars 2021 auraient déjà dû conduire le contrôlé à effectuer des investigations sur les mesures techniques et organisationnelles mises en place en interne, ainsi qu'auprès de son sous-traitant.
54. Or, comme les [données] de la réclamante ont encore une fois été transférées par son sous-traitant à la Société X le 15 février 2022, il s'avère que le contrôlé n'a pas procédé à un contrôle régulier des mesures techniques et organisationnelles mises en place par son sous-traitant. Il a même affirmé dans son courrier du 7 octobre 2022 que les données de la réclamante ont été supprimées des listes transmises à la Société X le 29 mars 2021 et n'ont plus été transmises par la suite. Néanmoins, une recherche du nom de la réclamante dans le fichier transmis par son sous-traitant à la Société X en février 2022, notamment par le raccourci clavier « Ctrl+f », aurait permis de voir que les [données] de la réclamante se trouvaient toujours dans ledit fichier.

55. Au vu de ce qui précède, la Formation Restreinte se rallie à l'avis du chef d'enquête et conclut qu'au début de l'enquête, le contrôlé n'a pas mis en œuvre des mesures techniques et organisationnelles appropriées lui permettant de vérifier le respect des dispositions du RGPD par son sous-traitant. Il a dès lors manqué à son obligation découlant de l'article 24.1 du RGPD.

II. 3. Sur l'amende et les mesures correctrices

1. Sur les principes

56. Conformément à l'article 12 de la loi du 1^{er} août 2018, 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. »

57. Conformément à l'article 48 de la loi du 1^{er} août 2018, la CNPD peut imposer des amendes administratives telles que prévues à l'article 83 du RGPD, sauf à l'encontre de l'État ou des communes.

58. L'article 83.1 du RGPD prévoit que chaque autorité de contrôle veille à ce que les amendes administratives imposées soient, dans chaque cas, effectives, proportionnées et dissuasives.

59. L'article 83.2 précise 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 ».

60. L'imposition des amendes administratives a été explicitée par le Groupe de Travail Article 29 dans ses « Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679 » adoptées le 3 octobre 2017. Ces lignes directrices ont été reprises et réapprouvées par le CEPD.²¹ La Formation Restreinte souligne que ces lignes directrices ont été complétées par les « Guidelines 04/2022 on the calculation of administrative fines under the GDPR » du CEPD dont la version 2.0 a été adoptée le 24 mai 2023.²²

61. 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 aux traitements de données faisant 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.

62. Néanmoins, les démarches effectuées par le contrôlé pour se mettre en conformité avec le RGPD en cours de la procédure d'enquête ou pour remédier aux manquements relevés par le chef d'enquête dans la communication des griefs, sont prises en compte par la Formation Restreinte dans le cadre des éventuelles mesures correctrices à prononcer et/ou de la fixation du montant d'une éventuelle amende administrative à prononcer.

²¹ Voir décision Endorsement 1/2018 du CEPD du 25 mai 2018, disponible sous : https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

²² Les lignes directrices sur le calcul des amendes ne sont actuellement que disponibles en anglais.

2. En l'espèce

2.1 Quant à l'imposition d'une amende administrative

63. Dans la communication des griefs, le chef d'enquête a proposé à la Formation Restreinte de prononcer à l'encontre du contrôlé une amende administrative d'un montant de 1.500 euros.²³

2.1.1 Sur l'opportunité de prononcer une amende administrative

64. Afin de décider s'il y a lieu d'imposer une amende administrative, la Formation Restreinte analyse les critères posés par l'article 83.2 du RGPD.

65. Quant à la nature et la gravité de la violation (article 83.2 a) du RGPD), elle rappelle en ce qui concerne le manquement à l'article 13 du RGPD que l'information sur les traitements de données à caractère personnel est une obligation essentielle pesant sur les responsables de traitement, afin que les personnes soient pleinement conscientes de l'utilisation qui sera faite de leurs données à caractère personnel, une fois celles-ci collectées. Un manquement à cet article du RGPD est ainsi constitutif d'une atteinte aux droits des personnes concernées. Le droit à l'information a par ailleurs été renforcé aux termes du RGPD, ce qui témoigne de leur importance toute particulière.

Quant au manquement à l'article 24 du RGPD, la Formation Restreinte tient à souligner que le principe de « responsabilité » (« accountability » en anglais) énoncé à l'article 5.2 du RGPD et développé à l'article 24 est également au cœur du RGPD et reflète le changement de paradigme induit par le RGPD, à savoir le passage d'un régime fondé sur des notifications et autorisations préalables par la CNPD à une plus grande imputabilité et responsabilité du responsable du traitement.

Par ailleurs, comme l'a rappelé le chef d'enquête, un tel manquement à l'article 24 du RGPD « *revient à vider de toute efficacité la législation en matière de protection des données à caractère personnel dès lors que le responsable du traitement ne s'assure pas que toutes les données qu'il transmet à son sous-traitant sont traitées en conformité avec le RGPD.* »²⁴

66. Quant au critère de durée (article 83.2.a) du RGPD), la Formation Restreinte constate que le manquement à l'obligation d'information a duré dans le temps, à tout le moins depuis la

²³ Communication des griefs, points 47 à 56 et 58.

²⁴ Communication des griefs, point 47.

mise en application du RGPD et jusqu'en octobre 2022, date à laquelle le document intitulé « CONDITIONS GENERALES DES SERVICES de la Société A » envoyé par le contrôlé au chef d'enquête en date du [...] octobre 2022 et disponible sur le site internet du contrôlé contenait un point spécifique sur la sous-traitance dans la partie plus globale concernant le traitement de données.

En effet, comme mentionné au point 34, elle ne dispose d'aucune documentation contenant une preuve attestant que le contrôlé a mis à jour ses conditions générales après l'entrée en application du RGPD et avant octobre 2022 en y intégrant des informations sur les destinataires des données à caractère personnel, et plus précisément sur le transfert des données à son sous-traitant la Société B.

En ce qui concerne la mise en place des mesures afin de s'assurer que son sous-traitant soit en conformité avec le RGPD conformément à l'article 24 du RGPD, notamment afin de vérifier que ce sous-traitant cesse de transférer les données à caractère personnel de la réclamante à la Société X, le contrôlé a confirmé lors de la séance de la Formation Restreinte du 27 avril 2023 que les transmissions irrégulières des [données] de la réclamante à la Société X étaient liées à un problème informatique interne et que cette mise à jour dans le système informatique de la Société A [...] aurait été faite en mars 2022.

Toutefois, aucune documentation soumise à la Formation Restreinte ne contient de preuve attestant que le contrôlé a dorénavant mis en place des mesures techniques et organisationnelles appropriées afin d'éviter que son sous-traitant transfère les données de la réclamante à la Société X, de sorte que la violation dure donc depuis du moins la résiliation du contrat de la réclamante en date du 30 juin 2019, date à partir de laquelle la Société B, en tant que sous-traitant du contrôlé, aurait dû cesser de transférer les données à caractère personnel de la réclamante à la Société X et ce du moins jusqu'en février 2022.

67. Quant au nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi (article 83.2 a) du RGPD), la Formation Restreinte constate en ce qui concerne le manquement à l'obligation d'informer les personnes concernées, que la réclamante n'avait pas l'information que ses données à caractère personnel traitées dans le cadre de son abonnement de la Société A étaient transférées depuis 2017 à la Société B en tant que sous-traitant du contrôlé. Elle se rallie au chef d'enquête en ce sens que « *cette absence d'information a eu pour conséquence que la réclamante a d'abord contacté une société tierce à la présente enquête et a mis du temps à comprendre quelles étaient les entités à l'origine du transfert de ses données à caractère personnel à la Société X afin de faire figurer ses [données sur le site] de la Société X. En outre, cette absence d'information*

concerne toutes les personnes ayant ou ayant eu un abonnement de la Société A depuis que le Contrôlé a conclu un contrat de sous-traitance avec la Société B. »²⁵

Au 31 décembre 2018, le nombre d'abonnés de la Société A était de [...] personnes, tandis qu'il n'était plus que de [...] au 31 décembre 2022. La Formation Restreinte est donc d'avis que tous ces clients sont des personnes concernées par le manquement à l'article 13 du RGPD.

Quant au manquement à l'obligation pour un responsable du traitement de mettre en œuvre des mesures techniques et organisationnelles appropriées lui permettant de vérifier le respect des dispositions du RGPD par son sous-traitant, la réclamante est l'unique personne connue de la CNPD comme ayant été affectée par les manquements au RGPD par le contrôlé.

68. Quant à la question de savoir si les manquements ont été commis délibérément ou par négligence (article 83.2.b) du RGPD), la Formation Restreinte rappelle que l'« *intention* » c'est-à-dire une infraction commise délibérément, comprend à la fois la connaissance et la volonté en rapport avec les caractéristiques d'une infraction, tandis que « *non délibéré* » (par négligence) signifie qu'il n'y a pas eu d'intention de commettre la violation, bien que le responsable du traitement ou le sous-traitant n'ait pas respecté l'obligation de diligence qui lui incombe en vertu de la législation.

La Formation Restreinte constate en l'espèce qu'elle ne dispose d'aucune preuve attestant que le contrôlé a mis à jour ses conditions générales après l'entrée en application du RGPD et avant octobre 2022 en y intégrant des informations sur les destinataires des données à caractère personnel. Par ailleurs, des transmissions irrégulières des données de la réclamante par le sous-traitant du contrôlé à la Société X pour publication [sur son site] ont eu lieu en 2020, 2021, ainsi qu'en février 2022.

Alors que la Formation Restreinte est d'avis que les faits et les manquements constatés ne traduisent pas une intention délibérée de violer le RGPD dans le chef du contrôlé, elle estime néanmoins que les manquements ont été commis par négligence.

69. Quant aux mesures prises par le contrôlé pour atténuer le dommage subi par les personnes concernées (article 83.2.c) du RGPD), la Formation Restreinte tient compte des

²⁵ Communication des griefs, point 49

mesures prises par le contrôlé et renvoie au Chapitre II.3, Section 2.2 de cette décision pour les explications y afférentes.

70. Elle relève aussi que si plusieurs mesures ont été mises en place par le contrôlé afin de remédier en totalité ou en partie à certains manquements, celles-ci n'ont été adoptées qu'à la suite du lancement de l'enquête par les agents de la CNPD en date du 23 août 2022²⁶ (voir aussi le point 61 de la présente décision).
71. 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 bonne coopération avec les agents de la CNPD en charge de l'enquête.
72. Quant aux catégories de données à caractère personnel concernées par la violation (article 83.2. g) du RGPD), il s'agit [des données]de la réclamante transféré[e]s illicitement et à plusieurs reprises par le sous-traitant du contrôlé à la Société X pour figurer [sur son site internet].
73. Quant à la manière dont la CNPD a eu connaissance de la violation (article 83.2 h) du RGPD), la CNPD a été informée des faits constitutifs de la violation dans le cadre de la réclamation introduite par la réclamante.
74. 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.
75. 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 13.1.e) et 24.1 du RGPD.

2.1.2. Sur le montant de l'amende

76. Le contrôlé est une société [...]. Il a indiqué avoir réalisé un chiffre d'affaires net de [...] euros et un résultat net de [...] euros pour l'année 2021.²⁷ Lors de la séance de la Formation Restreinte du 27 avril 2023, le contrôlé a précisé que les comptes annuels pour 2022 n'ont pas encore été finalisés.

²⁶ Envoi de l'ouverture de l'enquête avec les constats initiaux.

²⁷ Voir le courrier du 7 octobre 2022 dans lequel le contrôlé a indiqué ce qui suit [...].

[...].²⁸ Au 31 décembre 2018, le nombre d'abonnés de la Société A était de [...] personnes, tandis qu'il n'était plus que de [...] au 31 décembre 2022.²⁹

77. 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 maximal fixé pour la violation la plus grave. Dans la mesure où un manquement aux articles 13.1.e) et 24.1 du RGPD est reproché au contrôlé, le montant maximum de l'amende pouvant être retenu s'élève à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu, conformément à l'article 83.5 du RGPD.

78. Au regard de la responsabilité du contrôlé, de ses capacités financières et des critères pertinents de l'article 83.2 du RGPD évoqués ci-avant à la section « 2.1.1 Sur l'opportunité de prononcer une amende administrative », la Formation Restreinte considère que le prononcé d'une amende de mille cinq cents (1.500) euros apparaît à la fois effectif, proportionné et dissuasif, conformément aux exigences de l'article 83.1 du RGPD.

2.2 Quant à la prise de mesures correctrices

79. Dans la communication des griefs³⁰ le chef d'enquête « propose à la Formation Restreinte de prendre les mesures correctrices suivantes, endéans un délai de 1 mois à compter de la notification au Contrôlé de la décision prise par la Formation Restreinte :

« - Rappeler à l'ordre le responsable du traitement quant à son obligation d'information des personnes concernées, conformément à l'article 13 du RGPD ;

- Ordonner au responsable du traitement de mettre en place des mesures afin de s'assurer que son sous-traitant soit en conformité avec le RGPD, notamment afin de vérifier que ce sous-traitant cesse de transférer les données à caractère personnel de la Réclamante à la Société X »

80. Quant aux mesures correctrices proposées par le chef d'enquête et par référence au point 62 de la présente décision, la Formation Restreinte prend en compte les démarches effectuées par le contrôlé afin de se conformer aux dispositions des articles 13.1.e) et 24.1 du RGPD, telles que détaillées dans ses courriers du 7 octobre 2022 et du 28 novembre 2022. Plus particulièrement, elle prend note des faits suivants :

²⁸ Courrier du contrôlé à la CNPD en date du 28 novembre 2022.

²⁹ Courrier du contrôlé à la CNPD en date du 11 janvier 2022.

³⁰ Communication des griefs, points 42 à 45 et 54.

- Quant à la mesure correctrice proposée par le chef d'enquête reprise au premier tiret du point 79 de la présente décision concernant le rappel à l'ordre du responsable du traitement quant à son obligation d'information des personnes concernées, conformément à l'article 13 du RGPD, le contrôlé a envoyé par courrier du 7 octobre 2022 les conditions générales de la Société A actuellement en vigueur.

Dans la communication des griefs, le chef d'enquête a acté que « *[d]ésormais, dans les conditions générales de vente des services de la Société A figure l'information selon laquelle les données à caractère personnel des abonnées de la Société A sont transférées à la Société B* »

La Formation Restreinte constate en effet que le document intitulé « CONDITIONS GENERALES DES SERVICES de la Société A » envoyé par le contrôlé au chef d'enquête en date du [...] octobre 2022 et disponible sur le site internet du contrôlé contient un point spécifique sur la sous-traitance dans la partie plus globale concernant le traitement de données.

Néanmoins, comme mentionné au point 34, elle ne dispose d'aucune documentation contenant une preuve attestant que le contrôlé a mis à jour ses conditions générales après l'entrée en application du RGPD et avant octobre 2022 en y intégrant des informations sur les destinataires des données à caractère personnel, et plus précisément sur le transfert des données à son sous-traitant la Société B. Par contre, depuis au moins le [...] octobre 2022, les abonnés du contrôlé sont informés sur ce point.

Pour ces raisons, la Formation Restreinte estime qu'il y a lieu de prononcer la mesure correctrice proposée par le chef d'enquête à cet égard et reprise au premier tiret du point 79 de la présente décision et de rappeler à l'ordre le contrôlé pour avoir violé l'article 13.1. e) du RGPD.

- Quant à la mesure correctrice proposée par le chef d'enquête reprise au deuxième tiret du point 79 de la présente décision concernant la mise en place des mesures afin de s'assurer que son sous-traitant soit en conformité avec le RGPD, notamment afin de vérifier que ce sous-traitant cesse de transférer les données à caractère personnel de la réclamante à la Société X, le contrôlé a confirmé lors de la séance de la Formation Restreinte du 27 avril 2023 que les transmissions irrégulières des [données] de la réclamante à la Société X étaient liées à un problème informatique interne, car au

moment où l'abonnement de la réclamante avec la Société A a été résilié en 2019, l'inscription dans le fichier des clients [...] n'a pas été supprimée automatiquement. D'après le contrôlé, cette mise à jour dans le système informatique de la Société A [...] n'aurait été faite qu'en mars 2022.

Toutefois, aucune documentation soumise à la Formation Restreinte ne contient de preuve attestant que le contrôlé a dorénavant mis en place des mesures techniques et organisationnelles appropriées lui permettant de vérifier le respect des dispositions du RGPD par son sous-traitant afin d'éviter que ce dernier transfère de nouveau les données de la réclamante à la Société X.

En considération des mesures de mise en conformité insuffisantes prises par le contrôlé en l'espèce et du point 62 de la présente décision, la Formation Restreinte estime dès lors qu'il y a lieu de prononcer la mesure correctrice proposée par le chef d'enquête à cet égard et reprise au deuxième tiret du point 79 de la présente décision.

Compte tenu des développements qui précèdent, la Commission nationale siégeant en formation restreinte, après en avoir délibéré, décide :

- de retenir les manquements aux articles 13.1. e) et 24.1 du RGPD ;
- de prononcer à l'encontre de la « Société A » une amende administrative d'un montant de mille cinq cents (1.500) euros au regard des manquements aux articles 13.1. e) et 24.1 du RGPD ;
- de prononcer à l'encontre de la « Société A » une injonction de mettre en conformité les traitements avec les obligations résultant de l'article 24.1 du RGPD, dans un délai de deux mois suivant la notification de la décision de la Formation Restreinte, et, en particulier, mettre en place des mesures techniques et organisationnelles appropriées lui permettant de vérifier que son sous-traitant la Société B cesse de transférer les données à caractère personnel de la réclamante à la Société X ;
- de prononcer à l'encontre de la « Société A » un rappel à l'ordre pour avoir violé l'article 13.1. e) du RGPD.

Belvaux, le 5 juillet 2023.

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

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Marc Lemmer
Commissaire

Indication des voies de recours

La présente décision administrative peut faire l'objet d'un recours en réformation dans les trois mois qui suivent sa notification. Ce recours est à porter devant le tribunal administratif et doit obligatoirement être introduit par le biais d'un avocat à la Cour d'un des Ordres des avocats.