

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

Délibération n° 6FR/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 B [...] avait transféré les données à caractère personnel de la réclamante à la Société A 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 décidé d'ouvrir une enquête auprès des sociétés Société B, Société C et Société A 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 Commission nationale 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 [...] des statuts coordonnés du [...].

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 B vers la/les société(s) A et/ou 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 32.1 du RGPD (obligation de

garantir une sécurité appropriée) et par l'article 31 du RGPD (obligation de coopération avec l'autorité de contrôle).

Le chef d'enquête a proposé à la Formation Restreinte d'adopter trois mesures correctrices différentes, ainsi que d'infliger au contrôlé une amende administrative d'un montant de 5.330 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 (ci-après « lignes directrices 07/2020 ») 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

13. Par ailleurs, le CEDP a précisé dans les lignes directrices susmentionnées qu'une « *nouvelle caractéristique distincte du RGPD réside dans les dispositions imposant directement des obligations aux sous-traitants. [...] À cet égard, le [CEPD] estime que l'article 28, paragraphe 3, du RGPD, tout en imposant un contenu spécifique au contrat nécessaire que doivent conclure le responsable du traitement et le sous-traitant, impose des obligations directes aux sous-traitants, notamment l'obligation d'aider le responsable du traitement à garantir le respect des règles.* »³

14. De même, il en ressort que tant « *les responsables du traitement que les sous-traitants peuvent se voir infliger des amendes en cas de non-respect des obligations imposées par le RGPD qui les concernent et tous deux rendent compte directement aux autorités de contrôle en vertu des obligations de tenir à jour et de fournir les documents appropriés sur demande, de coopérer aux enquêtes et de se conformer aux injonctions administratives. Dans le même temps, il convient de rappeler que les sous-traitants doivent toujours se conformer aux instructions du responsable du traitement et agir uniquement selon celles-ci.* »⁴

2. En l'espèce

15. Par courriel du 21 juillet 2021 le contrôlé a expliqué que la Société B [...] »

16. Suite à des questions supplémentaires de la part du chef d'enquête⁵, le contrôlé a informé ce dernier dans un courrier du 6 octobre 2021⁶ de l'existence d'un contrat de collaboration conclu entre la Société C et la Société A fixant les conditions de fonctionnement et les opérations de la Société B, ainsi que les droits et obligations des parties.⁷ Il y est indiqué que « *la Société A ayant entre autre, pour mission de gérer/modifier/supprimer les [...] [listes des abonnés] de la Société B.* » Le contrôlé a conclu dans ledit courrier que « *la*

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 CEPD, Lignes directrices 07/2020, point 93.

⁴ CEPD, Lignes directrices 07/2020, point 9.

⁵ Voir courriel du 28 juillet 2021.

⁶ Voir pièce 9 annexée aux constats initiaux.

⁷ Ledit contrat de collaboration se trouve en annexe 4 de la réponse du contrôlé aux constats initiaux du 7 octobre 2022 et est intitulé : « Accord de collaboration entre les actionnaires de la Société B »

qualité de responsable de traitement des données à caractère personnel est attribuée aux deux parties. La Société C et la Société A étant coresponsable de traitement. »

17. Par contre, par courrier du 7 octobre 2022, le contrôlé s'est montré « *étonné de la réponse qui vous a été faite dans le courrier du 6 octobre 2021 (pièce numéro 9) dans laquelle la salariée affirme que la Société A serait coresponsable de traitement avec la Société C. En effet, la Société A est bien sous-traitant pour le compte de la Société B. Nous vous prions de nous excuser pour ces réponses douteuses. [...] . »*

En annexe du courrier précité se trouvait un document intitulé « *AVENANT AU CONTRAT DE SOUS-TRAITANCE CONCLU ENTRE LES SOCIETES « B » ET A » PORTANT SUR LE TRAITEMENT DES DONNEES CONFORMEMENT AU REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES (UE) 2016/679 DU 27 AVRIL 2016 APPLICABLE A COMPTER DU 25 MAI 2018 »* (ci-après : le « *contrat de sous-traitance* »).

18. La Formation Restreinte constate que l'article [...] dudit contrat de sous-traitance décrit en effet les tâches du contrôlé en sa fonction de sous-traitant de la Société B de la façon suivante :

[Le contrôlé] est autorisé[e] à traiter pour le compte [de la Société B] les données à caractère personnel nécessaires pour que [...] [le contrôlé] puisse gérer l'aspect administratif des abonnements générés par [la Société B].

La nature des opérations réalisées sur les données est :

- *Consultation/traitement des données personnelles*
- *Sauvegarde temporaire des données*
- *Import des données personnelles*
- *Modification des données*
- *Tout autre usage nécessaire à la maintenance du service.*

Les finalité(s) du traitement sont la gestion administrative des abonnements générés par [la Société B] et la fourniture de services aux clients [de la Société B].

Les données à caractère personnel traitées sont toutes les données d'identification des clients [de la Société B] (nom, prénom, adresse complète, numéro de téléphone, copie de contrat) ainsi que les données nécessaires à la gestion du contrat d'abonnement du client [de la Société B].

Les catégories de personnes concernées sont tous les clients ayant souscrit un contrat [Société B]. »

19. Comme la réclamante a souscrit en date du 27 avril 2015⁸ un contrat d'abonnement avec la Société B, cette dernière est à considérer comme responsable du traitement des données à caractère personnel de la réclamante dans le cadre dudit contrat, tandis que le contrôlé agit dans ce contexte spécifique comme sous-traitant de la Société B ayant pour mission de gérer/modifier/supprimer pour le compte de ladite société les [listes d'abonnés] conformément au contrat de sous-traitance précité.
20. Lors de la séance de la Formation Restreinte du 27 avril 2023, le contrôlé a confirmé les qualités précitées de la Société B et de la Société A, 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, des membres du personnel du contrôlé auraient accès au système informatique de la Société B pour faire les opérations nécessaires pour son compte, notamment afin de générer un fichier [...] avec les clients souhaitant apparaître [sur le site internet] de la Société X, 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 de garantir une sécurité appropriée

1. Sur les principes

21. En vertu de l'article 32.1 du RGPD et « *compte tenu de l'état des connaissances, des coûts de mise en oeuvre et 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 et le sous-traitant mettent en oeuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque y compris entre autres, selon les besoins:*

a) la pseudonymisation et le chiffrement des données à caractère personnel ;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

⁸ Voir pièce 2 annexée à la communication des griefs.

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement. »

22. A noter que le CEDP a précisé dans les lignes directrices 07/2020 que le « *RGPD établit des obligations directement et spécifiquement applicables aux sous-traitants* » et qu'un « *sous-traitant peut être tenu responsable ou se voir infliger une amende en cas de non-respect de ces obligations ou s'il outrepassé ou enfreint les instructions légales du responsable du traitement.* »⁹ Une de ces obligations est précisément qu'un sous-traitant doit mettre en œuvre les mesures techniques et organisationnelles appropriées conformément à l'article 32 du RGPD.

2. En l'espèce

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

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] avaient été publiées [...] sur le site internet de la Société X et que lesdites [données] ont été transférées par le contrôlé à la Société X pour publication [sur ledit site]. En date du 19 octobre 2020, la Société X a confirmé à la réclamante que ses données seraient supprimées de son site internet.

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 le contrôlé pour publication [sur son site].¹⁰

24. Par courrier du 1^{er} juin 2021, le contrôlé a précisé avoir pour « *mission de gérer/modifier/supprimer les [listes des abonnés] au nom de la Société B* », d'une part, et 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'autre part.

Par ailleurs, dans le même courrier le contrôlé a expliqué que, comme la réclamante n'était plus abonnée auprès de la Société B depuis le 30 juin 2019, « *ses [données] n'auraient*

⁹ CEPD, Lignes directrices 07/2020, point 74.

¹⁰ Voir constats 1 à 7 des constats initiaux.

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. »

25. Or, suite à un nouvel 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 avait eu lieu suite à un transfert desdites [données] par le contrôlé à la Société X en février 2022.¹¹

26. Par courrier du 7 octobre 2022, le contrôlé a reconnu que la Société X lui avait déjà demandé la suppression des données de la réclamante *« le 19 octobre 2020 sans réponse de notre part avec relance le 29 mars 2021. Nous avons fait droit à la demande à cette date et les données de la cliente n'ont plus été transmises à la Société X par la suite. »*

Dans le même courrier, le contrôlé a par ailleurs formellement contesté avoir à nouveau transféré les données de la réclamante à la Société X en février 2022 et a insisté *« que depuis le 29 mars 2021 [la réclamante] n'est plus sur les listes transmises par la Société A à la Société X, en atteste le fichier envoyé à la Société X le 15 avril 2021 que nous pouvons vous transmettre au besoin. »*

27. Suite à cette contestation, le chef d'enquête a demandé au contrôlé par courrier du 6 décembre 2022 *« de nous transmettre les communications telles que transmises, dans leur forme exacte et sans la moindre altération, par la Société A à la Société X des données des abonnés de la Société B devant figurer [sur le site] de la Société X, aux dates suivantes : Communications d'avril et mai 2021 ; Communication du 23 février 2022 et des mois de mars, avril, mai, juin, juillet, août, septembre et octobre 2022. »*

28. Le contrôlé a envoyé les documents demandés par courriel du 14 décembre 2022.

29. Dans la communication des griefs du 25 janvier 2023, le chef d'enquête a acté que la Société X a reçu du contrôlé les données de la réclamante afin de les faire figurer [sur son site] en 2020 et 2021, alors que l'abonnement de la Société B de la réclamante a pris fin le 30 juin 2019, *« date à partir de laquelle le Contrôlé, en tant que sous-traitant de la Société B, aurait dû cesser de transférer les données à caractère personnel de la Réclamante à la Société X »*¹²

¹¹ Voir constats 16 et 17 des constats initiaux.

¹² Communication des griefs, points 20 et 21.

30. 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 B tel que transmis en février 2022 par le contrôlé à la Société X, afin que ces personnes figurent [sur le site internet] de la Société X, d'une part, et qu'une recherche « Ctrl+f » dans ledit fichier [...] « *permet pourtant de voir que les données de la Réclamante sont bien présentes parmi les données des abonnés de la Société B à faire figurer [sur le site] de la Société X* », d'autre part. ¹³

Ainsi, le chef d'enquête a retenu que « *les conditions de l'article 32, paragraphe 1, du RGPD n'ont pas été respectées, le Contrôlé n'ayant pas mis en œuvre les mesures techniques et organisationnelles appropriées d'une part, afin de garantir la confidentialité des données à caractère personnel de la Réclamante et éviter ainsi que celles-ci ne soient transférées à la Société X suite à la résiliation de son contrat d'abonnement de la Société B et, d'autre part, afin de tester, analyser et évaluer régulièrement l'efficacité desdites mesures.* »¹⁴

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

32. Par courriel du 1^{er} juin 2021, le contrôlé a avoué qu'il n'aurait pas dû transférer les données de la réclamante à la Société X et qu'il s'agissait d'une « *erreur de paramétrage interne* », tandis que dans un courrier du 7 octobre 2022, il « *pens[ait] que ces manquements sont advenus suite à des erreurs humaines successives. En effet, la période du contentieux est située au cœur de la crise liée au Covid-19. Nos équipes ont souvent dû travailler en sous-effectif durant la crise suite aux nombreux arrêts de travail, isolements et congés pour raisons familiales. Par ailleurs et devant l'urgence de la situation, nous avons dû modifier*

¹³ Communication des griefs, points 24 et 25.

¹⁴ Communication des griefs, point 26.

notre organisation de travail et mettre en place dans la précipitation un roulement de présence dans l'entreprise. »

33. Dans ce même courrier, le contrôlé a reconnu que la Société X lui avait déjà demandé la suppression des données de la réclamante *« le 19 octobre 2020 sans réponse de notre part avec relance le 29 mars 2021. Nous avons fait droit à la demande à cette date et les données de la cliente n'ont plus été transmises à la Société X par la suite. »*
34. 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 B avait été résilié, soit en 2019, l'inscription dans le fichier des personnes souhaitant apparaître [sur le site] de la Société X n'avait pas été supprimée automatiquement. D'après le contrôlé, cette mise à jour dans le système informatique de la Société B [...] n'aurait été faite qu'en mars 2022.
35. Indépendamment des raisons qui ont menées à ces transmissions irrégulières des [données] de la réclamante à la Société X, la Formation Restreinte constate en premier lieu qu'il ressort des constatations qui précèdent que le contrôlé ne disposait pas de procédure spécifique établie afin de tester et analyser régulièrement si sur les listes de [données] transmises à la Société X ne figuraient pas des abonnés qui ont soit résilié leur contrat d'abonnement avec la Société B, soit demandé à ne plus figurer [sur le site internet].
36. En deuxième lieu, la Formation Restreinte relève 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 dû conduire le contrôlé à effectuer des investigations sur son système de sécurité. Or, comme les [données] de la réclamante ont encore une fois été transférées à la Société X le 15 février 2022, la Formation Restreinte considère que les mesures déployées pour garantir la sécurité des données en l'espèce étaient insuffisantes et ne respectaient pas les exigences minimales nécessaires en termes de sécurité.

37. 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'enquête¹⁵, le contrôlé a manqué à son obligation découlant de l'article 32.1 du RGPD.

38. Quant aux mesures prises par le contrôlé après le début de l'enquête, la Formation Restreinte y revient au point 58, ainsi qu'au Chapitre II.3. Section 2.2. de cette décision.

B. Sur le manquement lié à l'obligation de coopération avec l'autorité de contrôle

1. Sur les principes

39. Selon l'article 31 du RGPD, « *[l]e responsable du traitement et le sous-traitant ainsi que, le cas échéant, leurs représentants, coopèrent avec l'autorité de contrôle, à la demande de celle-ci, dans l'exécution de ses missions.* »

40. Comme mentionné au point 14 de la présente décision, le CEDP a précisé dans ses lignes directrices 07/2020 qu'un « *sous-traitant peut être tenu responsable ou se voir infliger une amende en cas de non-respect de ces obligations ou s'il outrepassé ou enfreint les instructions légales du responsable du traitement.* »¹⁶ Une de ces obligations est précisément qu'un sous-traitant doit coopérer « *avec l'autorité de contrôle, à la demande de celle-ci, dans l'exécution de ses missions* » comme exigé par l'article 31 précité du RGPD.

2. En l'espèce

41. Il ressort de la communication des griefs que dans le cadre de la réclamation introduite par la réclamante en date du 10 mars 2021, la CNPD a dû contacter le contrôlé à plusieurs reprises en 2021 et 2022 et lui a même envoyé des courriers de rappel, car il « *ne répondait pas dans les délais aux questions qui lui étaient posées. Cela a notamment été le cas d'un courrier de la CNPD du 28 juillet 2021 qui a fait l'objet d'un rappel le 10 septembre 2021, ainsi que d'un courrier de la CNPD du 20 janvier 2022 qui a fait l'objet d'un rappel en date du 9 mars 2022 et est resté sans réponse. L'absence de réponse du Contrôlé à ce dernier courrier, qui soulevait de nombreuses problématiques, a en partie motivé l'ouverture de la présente enquête.* »¹⁷

¹⁵ 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.

¹⁶ CEPD, Lignes directrices 07/2020, point 74.

¹⁷ Communication des griefs, points 29 et 30.

42. Par ailleurs, le chef d'enquête a acté que « *de nombreux propos tenus par le Contrôlé dans le cadre de la Réclamation ont ensuite été réfutés dans le courrier du Contrôlé du 7 octobre 2022 en réponse aux Constats Initiaux (PIECE 4). Le Contrôlé a en effet expliqué que les réponses avaient été formulées par un ou des salarié(s) et n'avaient pas fait l'objet d'une validation par la direction avant leur envoi à la CNPD.* »¹⁸

43. Finalement, alors que le contrôlé avait pourtant assuré dans son courrier du 7 octobre 2022 en réponse aux constats initiaux que des mesures avaient été prises à partir du 29 mars 2021, le chef d'enquête a noté que les données de la réclamante avaient à nouveau été transférées par le contrôlé à la Société X en février 2022. D'après le chef d'enquête, il « *est étonnant que le Contrôlé n'ait pas mis en œuvre les mesures les plus simples, telles qu'une action de recherche « Ctrl+f » dans ses fichiers, afin d'apporter une réponse exacte aux questions soulevées par les agents de la CNPD en charge de l'enquête. Une telle inaction peut laisser penser que le Contrôlé a cherché, de façon intentionnelle, à cacher aux agents de la CNPD en charge de l'enquête le fait que les données à caractère personnel de la Réclamante aient à nouveau été transférées à la Société X en date du 23 février 2022.* »

Pour les raisons qui précèdent, le chef d'enquête a retenu « *que les conditions de l'article 31 du RGPD n'ont pas été respectées, le Contrôlé ayant, d'une part, cessé de répondre aux questions de la CNPD dans le cadre du traitement de la Réclamation introduite par la Réclamante et, d'autre part, donné des réponses fausses bien que facilement vérifiables dans le cadre de la présente enquête.* »¹⁹

44. La Formation Restreinte rappelle que tant les responsables du traitement que les sous-traitants « *rendent compte directement aux autorités de contrôle en vertu des obligations de tenir à jour et de fournir les documents appropriés sur demande, de coopérer aux enquêtes et de se conformer aux injonctions administratives.* »²⁰

45. Elle note dans ce contexte que certains courriers, voire courriels de la CNPD adressés au contrôlé dans le cadre de la gestion de la réclamation sont restés sans réponse.²¹

¹⁸ Communication des griefs, points 31.

¹⁹ Communication des griefs, points 33 et 34.

²⁰ CEPD, Lignes directrices 07/2020, point 9.

²¹ Voir le courrier de la CNPD du 28 juillet 2021 qui a fait l'objet d'un rappel le 10 septembre 2021, ainsi qu'un courrier de la CNPD du 20 janvier 2022 qui a fait l'objet d'un rappel en date du 9 mars 2022. Il s'agit des pièces 7,8,10 et 14 annexées aux constats initiaux.

46. Dans son courrier du 7 octobre 2022 suite à l'envoi des constats initiaux par le chef d'enquête, le contrôlé a expliqué que les « *pièces numéros 10 et 14 font références à des mails envoyés par vos services sur notre adresse [...], lesquels sont restés sans réponse de notre part. Nous prenons connaissance de ces manquements à la lecture du dossier que vous nous avez transmis et souhaitons-nous en excuser. Après analyse interne, cette situation découle de démissions successives au sein de notre service contentieux. En effet, le service est composé de deux juristes. L'un d'eux a quitté nos effectifs [fin] 2021 et l'autre, chargé de la reprise du dossier a quitté nos effectifs [début] 2022.* »
47. Lors de la séance de la Formation Restreinte du 27 avril 2023, le contrôlé a même formellement contesté l'allégation du chef d'enquête qu'il n'aurait pas voulu coopérer avec la CNPD ou qu'il aurait essayé de cacher quelque chose, tout en confirmant que les [données] de la réclamante étaient de nouveau dans le fichier transmis à la Société X en février 2022 dû à un problème informatique interne.
48. La Formation Restreinte estime tout d'abord qu'une société qui utilise pour son service contentieux une adresse mail générique comme « [...] », indiquée d'ailleurs en bas de page des courriers du contrôlé, doit s'assurer que les courriels à destination de ladite adresse soient lus régulièrement, même en cas de démission d'une personne ayant travaillé dans le service en cause.
49. Elle s'étonne que le contrôlé n'a par ailleurs pas contrôlé que les [données] de la réclamante ne figuraient plus dans le fichier transmis à la Société X en février 2022 avant de contester formellement cette allégation dans son courrier du 7 octobre 2022 tout en confirmant « *que depuis le 29 mars 2021 Madame [...] n'est plus sur les listes transmises par la Société A à la Société X.* » Or, comme le contrôlé a lui-même transmis, uniquement une semaine après la demande du chef d'enquête, notamment ledit fichier de février 2022 prouvant que les [données] de la réclamante s'y trouvaient de nouveau, la Formation Restreinte ne partage pas l'avis du chef d'enquête selon lequel le contrôlé « *a cherché, de façon intentionnelle, à cacher aux agents de la CNPD en charge de l'enquête le fait que les données à caractère personnel de la Réclamante aient à nouveau été transférées à la Société X en date du 23 février 2022.* »²², mais estime qu'il s'agit d'une négligence de sa part.
50. En ce qui concerne l'interprétation erronée de la qualité du contrôlé à l'égard des traitements en cause exprimée par une salariée dans un courrier du 6 octobre 2021 et

²² Communication des griefs, point 33.

rectifiée par le contrôlé dans son courrier du 7 octobre 2022, la Formation Restreinte estime que ce malentendu témoigne d'un manque de communication interne et non pas d'une non-coopération du contrôlé avec la CNPD.

51. Néanmoins, comme la CNPD a dû contacter le contrôlé à plusieurs reprises en 2021 et 2022 et lui a même envoyé des courriers de rappel sans réponse, la Formation Restreinte se rallie sur ce point à l'avis du chef d'enquête et conclut qu'au début de l'enquête, l'article 31 du RGPD n'était pas respecté par le contrôlé, car il a manqué à son obligation de coopération avec l'autorité de contrôle, à savoir, la CNPD.

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

1. Sur les principes

52. 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. »

53. 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.

54. 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.

55. 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 ».*

56. 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 CEPD²³. 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 2023.²⁴

57. 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.

58. 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

²³ 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 Les lignes directrices sur le calcul des amendes ne sont actuellement que disponibles en anglais.

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.

2. En l'espèce

2.1 Quant à l'imposition d'une amende administrative

59. Dans la communication des griefs, le chef d'enquête propose à la Formation Restreinte de prononcer à l'encontre du contrôlé une amende administrative d'un montant de 5.330 euros.²⁵

2.1.1 Sur l'opportunité de prononcer une amende administrative

60. 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.

61. 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 32.1 du RGPD, que face aux risques représentés par les violations de données à caractère personnel, le législateur européen a entendu renforcer les obligations des responsables de traitement en matière de sécurité des traitements. Ainsi, selon le considérant (83) du RGPD et afin de « *de garantir la sécurité et de prévenir tout traitement effectué en violation du présent Règlement, il importe que le responsable du traitement ou le sous-traitant évalue les risques inhérents au traitement et mette en oeuvre des mesures pour les atténuer, telles que le chiffrement. Ces mesures devraient assurer un niveau de sécurité approprié, y compris la confidentialité, compte tenu de l'état des connaissances et des coûts de mise en oeuvre par rapport aux risques et à la nature des données à caractère personnel à protéger. [...].* »

Or, comme les données à caractère personnel de la réclamante ont été transférées de manière illicite en 2020, 2021, ainsi qu'en février 2022 par le contrôlé à la Société X, la Formation Restreinte estime qu'il n'a pas mesuré l'importance de la sécurisation des données personnelles contenues dans le système informatique du responsable du traitement auquel il a accès pour traiter pour son compte les données de la réclamante.

62. Quant au critère de durée (article 83.2.a) du RGPD), la Formation Restreinte constate que 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

²⁵ Communication des griefs, points 46 à 53 et 55.

à un problème informatique interne et que cette mise à jour dans le système informatique de la Société B [...], 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 de transférer les données de la réclamante à la Société X, de sorte que la violation dure donc depuis la résiliation du contrat de la réclamante en date du 30 juin 2019. A partir de cette date, le contrôlé en tant que sous-traitant du contrôlé, aurait dû cesser de transférer les données à caractère personnel de la réclamante à la Société X.

63. 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 que la réclamante est l'unique personne connue de la CNPD comme ayant été affectée par les manquements au RGPD par le contrôlé.

64. En ce qui concerne le dommage subi par la réclamante, le considérant (75) du RGPD précise qu'il ne s'agit pas uniquement de dommages physiques et matériels, mais aussi de préjudices moraux. En transmettant fréquemment et de manière illicite les données de la réclamante à la Société X afin de publication [sur son site], tout internaute avait accès à ses [données], sans qu'elle y a consenti. La réclamante a même été contactée à plusieurs reprises dans le cadre de démarchage téléphonique religieux.

65. 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 que des transmissions irrégulières des données de la réclamante par le contrôlé pour le compte de la Société B 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.

66. Quant aux mesures prises par le contrôlé pour atténuer le dommage subi par les personnes concernées (article 83.2.c), la Formation Restreinte tient compte des mesures prises par le contrôlé et renvoie au Chapitre II.3, Section 2.2 de cette décision pour les explications y afférentes.
67. 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 57 de la présente décision).
68. Quant au degré de responsabilité du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'il a mises en œuvre en vertu des articles 25 et 32 (article 83.2.d) du RGPD), la Formation Restreinte prend en compte que les données de la réclamante n'ont pas uniquement été transférées de manière illicite en 2020, mais aussi en 2021, ainsi qu'en février 2022. Par ailleurs, elle relève 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 dû conduire le contrôlé à effectuer des investigations sur son système de sécurité conformément à l'article 32 du RGPD, ce qu'il n'a pourtant pas fait.
69. 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 *« qu'il a été nécessaire, à plusieurs reprises dans le cadre de l'enquête, envoyer au Contrôlé des courriers et courriels de relance afin d'obtenir réponse à ses questions. »*²⁷
70. 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 contrôlé pour le compte de la Société B à la Société X pour figurer [sur son site internet].
71. 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.
72. 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.

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

²⁷ Communication des griefs, point 49.

73. 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 31 et 32.1 du RGPD.

2.1.2. Sur le montant de l'amende

74. Le contrôlé a indiqué avoir réalisé un chiffre d'affaires de [...] € pour l'année 2021, et un résultat net de [...] € pour l'année 2021.²⁸ Il dispose d'un effectif de plus de [...] collaborateurs [...], et de plus de [...] clients privés et professionnels.²⁹

75. 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 31 et 32.1 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, conformément à l'article 83.5 du RGPD.

76. 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 au chapitre « 2.1.1 Sur l'opportunité de prononcer une amende administrative », la Formation Restreinte considère que le prononcé d'une amende de deux mille cinq cents (2.500) 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

77. Dans la communication des griefs³⁰ le chef d'enquête a proposé à la Formation Restreinte d'adopter 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, sous peine d'astreinte à hauteur de 50 euros par jour de retard:*

« • *Ordonner au Contrôlé l'interdiction définitive du traitement des données à caractère personnel de la Réclamante consistant en un transfert desdites données à la Société X;*

²⁸ Voir le courrier du 7 octobre 2022 dans lequel le contrôlé a indiqué ce qui suit [...].

²⁹ Informations disponibles sur le site internet du contrôlé : [...].

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

- *Ordonner au Contrôlé de mettre en place des mesures techniques et organisationnelles suffisantes afin d'assurer la confidentialité des données à caractère personnel ainsi qu'une procédure visant à tester, analyser et évaluer régulièrement l'efficacité desdites mesures ;*
- *Rappeler à l'ordre le Contrôlé quant à son obligation de coopération avec la CNPD. »*

78. Quant aux mesures correctrices proposées par le chef d'enquête et par référence au point 58 de la présente décision, la Formation Restreinte prend en compte les démarches effectuées par le contrôlé afin de se conformer aux dispositions des articles 32.1 et 31 du RGPD, telles que détaillées dans ses courriers du 7 octobre 2022 et du 14 décembre 2022. Plus particulièrement, elle prend note des faits suivants :

- Quant à la mesure correctrice proposée par le chef d'enquête reprise au premier tiret du point 77 de la présente décision concernant l'interdiction définitive du traitement des données à caractère personnel de la réclamante consistant en un transfert desdites données à la Société X, le contrôlé a indiqué dans son courrier du 14 décembre 2022 avoir pris en compte la demande de la Société X visant à supprimer la réclamante des listes [...] et que dès lors, la réclamante « *a bien été sortie de nos listes dès le 28 mai 2021* ».

La Formation Restreinte constate toutefois, comme mentionné au point 31, que le contrôlé a fait parvenir dans ce même courrier du 14 décembre 2022, entre autres, le courriel et le fichier [...] envoyés le 15 février 2022 à la Société X contenant de nouveau les [données] de la réclamante.

Lors de la séance de la Formation Restreinte du 27 avril 2023, le contrôlé a confirmé que, contrairement aux affirmations précédentes, dans ledit 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 B a été terminé 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 B [...] n'aurait été faite qu'en mars 2022.

Elle constate en effet qu'au courrier du contrôlé du 14 décembre 2022 est annexé un courriel de la Société X du 8 mars 2022 demandant au contrôlé de ne plus inclure les [données] de la réclamante dans les listes [...], d'une part, ainsi que les fichiers transmis par le contrôlé à la Société X d'avril à octobre 2022 et qui ne contiennent plus les [données] de la réclamante, d'autre part.

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 afin d'éviter de transférer de nouveau pour le compte de la Société B 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 58 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 premier tiret du point 77 de la présente décision.

- Quant à la mesure correctrice proposée par le chef d'enquête reprise au deuxième tiret du point 77 de la présente décision concernant la mise en place des mesures techniques et organisationnelles suffisantes afin d'assurer la confidentialité des données à caractère personnel ainsi qu'une procédure visant à tester, analyser et évaluer régulièrement l'efficacité desdites mesures, 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 B [...] 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 mis en place une procédure spécifique afin de tester et analyser régulièrement si sur les listes de [données] qu'il transmet à la Société X pour le compte de la Société B ne figuraient pas des abonnés qui ont soit résilié leur contrat d'abonnement avec la Société B, soit demandé à ne plus figurer [sur le site] afin de garantir la sécurité des données et de respecter les exigences minimales nécessaires en termes de sécurité.

En considération des mesures de mise en conformité insuffisantes prises par le contrôlé en l'espèce et du point 58 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 premier tiret du point 77 de la présente décision.

- Quant à la mesure correctrice proposée par le chef d'enquête reprise au troisième tiret du point 77 de la présente décision concernant le rappel à l'ordre du contrôlé quant à son obligation de coopération avec la CNPD, la Formation Restreinte a constaté que la CNPD a dû contacter le contrôlé à plusieurs reprises en 2021 et 2022 et lui a même

envoyé des courriers de rappel sans réponse. Elle était dès lors d'avis qu'au début de l'enquête, l'article 31 du RGPD n'était pas respecté par le contrôlé, car il a manqué à son obligation de coopération avec l'autorité de contrôle, à savoir, la CNPD.

Pour ces raisons, 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 troisième tiret du point 77 de la présente décision et de rappeler à l'ordre le contrôlé pour avoir violé l'article 31 du RGPD.

- La Formation Restreinte estime par ailleurs qu'il n'y a pas lieu d'infliger une astreinte au contrôlé pour le contraindre à respecter ces mesures correctrices.

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

- de retenir les manquements aux articles 31 et 32.1 et du RGPD ;
- de prononcer à l'encontre de la « Société A » une amende administrative d'un montant de deux mille cinq cents (2.500) euros au regard des manquements aux articles 31 et 32.1 du RGPD ;
- de prononcer à l'encontre de la « Société A » une interdiction définitive de traitement des données à caractère personnel de la réclamante consistant en un transfert desdites données à la Société X ;
- de prononcer à l'encontre de la « Société A » une injonction de mettre en conformité les traitements avec les obligations résultant de l'article 32.1 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 suffisantes afin d'assurer la confidentialité des données à caractère personnel de la réclamante ainsi qu'une procédure visant à tester, analyser et évaluer régulièrement l'efficacité desdites mesures.
- de prononcer à l'encontre de la « Société A » un rappel à l'ordre pour avoir violé l'article 31 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.