Délibération SAN-2021-008 du 14 juin 2021

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Sanction
Date de publication sur Légifrance : Jeudi 17 juin 2021
Etat juridique : En vigueur

Délibération de la formation restreinte n°SAN-2021-008 du 14 juin 2021 concernant la société X

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de Monsieur Alexandre LINDEN, président, Monsieur Philippe-Pierre CABOURDIN, vice-président, Madame Anne DEBET, Madame Christine MAUGÜE et Monsieur Bertrand du MARAIS, membres ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données ;

Vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ;

Vu le code des postes et des communications électroniques ;

Vu la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 20 et suivants ;

Vu le décret no 2019-536 du 29 mai 2019 pris pour l'application de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération no 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2018-238C du 27 septembre 2018 de la présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification des traitements mis en œuvre par cet organisme ou pour le compte de la société [...] ;

Vu la décision de la présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte, en date du 19 décembre 2019 ;

Vu le rapport de Madame Valérie PEUGEOT, commissaire rapporteure, notifié à la société [...] le 2 octobre 2020 ;

Vu les observations écrites versées par la société [...] le 2 novembre 2020 ;

Vu la réponse de la rapporteure à ces observations notifiées le 24 novembre 2020 au conseil de la société ;

Vu les nouvelles observations écrites versées par le conseil de la société [...], reçues le 16 décembre 2020, ainsi que les observations orales formulées lors de la séance de la formation restreinte ;

Vu le document relatif au déploiement de la procédure d'archivage intermédiaire et d'anonymisation des données des prospects et clients de la société [...] versée par le conseil de la société [...] lors de la séance de la formation restreinte ;

Vu le procès-verbal de constat d'huissier réalisé le 5 février 2021 ainsi que son annexe, adressés par le conseil de la société au président de la formation restreinte et à la rapporteure le 10 février 2021 ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 28 janvier 2021 :

- Madame Valérie PEUGEOT, commissaire, entendue en son rapport ;

En qualité de représentants de la société [...] :

- […] ;

- […] ;

- […] ;

- […].

La société [...] ayant eu la parole en dernier ;

La formation restreinte a adopté le projet de décision suivant :

I. Faits et procédure

1. La société [...] (ci-après " la société ") est une société par actions simplifiée à associé unique créée en 2012. Son siège social est situé […]. Elle est présidée par la société Y, société par actions simplifiée, située […].

2. La société édite le site internet [...], qui est accessible en France, en Espagne depuis 2015, en Italie depuis 2016 et au Portugal depuis 2017. Il s'agit d'un site de ventes privées dédié au bricolage, au jardinage et à l'aménagement de la maison. Jusqu'au mois de […], les ventes étaient accessibles à condition d'avoir créé un compte sur le site. Depuis cette date, les ventes sont visibles sans condition préalable de création de compte. En revanche, pour effectuer un achat, il est toujours nécessaire de créer un compte sur le site [...]. En 2018, la société comptait […] utilisateurs en France, […] utilisateurs en Espagne, […] utilisateurs en Italie et […] utilisateurs au Portugal.

3. Elle a réalisé, en 2018, un chiffre d'affaires d'environ […] euros, pour un résultat net d'environ […] euros. En 2019, elle a réalisé un chiffre d'affaires d'environ […] euros pour un résultat net d'environ […] euros. En 2020, elle a réalisé un chiffre d'affaires d'environ […] euros, pour un résultat net d'environ […] euros. La société [...] employait, en 2018, environ 150 personnes.

4. Le 13 novembre 2018, en application de la décision no 2018-238C du 27 septembre 2018 de la présidente de la CNIL, une délégation de la CNIL a procédé à une mission de contrôle dans les locaux de la société. Cette mission avait pour objet de vérifier le respect par cette société de l'ensemble des dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après " le Règlement " ou " le RGPD ") et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après " la loi du 6 janvier 1978 modifiée " ou la loi " Informatique et Libertés ").

5. Le contrôle visait plus particulièrement les traitements de données à caractère personnel des clients et des prospects de la société. Les vérifications opérées ont notamment porté sur les durées de conservation des données à caractère personnel, l'information portée à la connaissance des personnes concernées s'agissant des traitements effectués par la société, le respect des demandes d'effacement des données à caractère personnel des personnes concernées, l'obligation d'assurer la sécurité des données ainsi que l'obligation de recueillir le consentement de la personne concernée à recevoir de la prospection commerciale par courrier électronique.

6. A l'issue du contrôle, le procès-verbal n°2018-238/1 a été notifié à la société [...] par courrier daté du 19 novembre 2018. La société a transmis aux services de la Commission, par courriel du même jour, les pièces complémentaires sollicitées à l'issue de la mission de contrôle.

7. Par courriel du 5 février 2019, la société a communiqué de sa propre initiative à la délégation plusieurs pièces complémentaires, notamment un document intitulé " Procédure de conservation des données à caractère personnel ".

8. Les investigations ayant permis d'établir le caractère transfrontalier du traitement concerné, la CNIL a informé le 27 août 2019, conformément à l'article 56 du RGPD, l'ensemble des autorités de contrôle européennes de sa compétence pour agir en tant qu'autorité de contrôle chef de file et a ainsi ouvert la procédure pour la déclaration des autorités concernées sur ce cas.

9. Le 27 septembre 2019, la présidente de la CNIL a soumis aux autorités concernées un projet de mise en demeure. À la suite de cette diffusion, trois autorités ont formulé des objections pertinentes et motivées au sens de l'article 60 du RGPD, demandant pour deux d'entre elles que le projet de mise en demeure soit modifié en un projet de sanction, et plus particulièrement d'amende administrative pour l'une de ces deux autorités. Au soutien de cette demande, les autorités concernées soulignaient notamment le nombre de manquements, le nombre de personnes concernées et la taille de la société.

10. Afin de compléter ses investigations, la CNIL a, le 6 février 2020, en application de la décision n° 2018-238C susvisée, procédé à une mission de contrôle en ligne de tout traitement accessible à partir du domaine [...].

11. Ce contrôle portait plus particulièrement sur les modalités d'information des personnes concernées sur le site web [...] et sur le dépôt de cookies sur le terminal des utilisateurs lors de leur arrivée sur ce site.

12. A la suite du contrôle, le procès-verbal n° 2018-238/2 a été notifié à la société [...] par courrier daté du 19 février 2020. La société a transmis aux services de la Commission, par courriels des 4 mars et 9 juillet 2020, les pièces complémentaires et les informations sollicitées à l'issue de la mission de contrôle.

13. Le 13 janvier 2021, une délégation de la CNIL a, en application de la décision n° 2018-238C susvisée, procédé à une nouvelle mission de contrôle en ligne de tout traitement accessible à partir du domaine [...]. La société ayant indiqué que des modifications avaient été apportées aux modalités de dépôt des cookies, il a été décidé de procéder à un nouveau contrôle afin de réactualiser les constats effectués le 6 février 2020.

14. A l'issue du contrôle, le procès-verbal n°2018-238/3 a été notifié à la société [...] par courrier daté du 14 janvier 2021. Par courriel du 26 janvier 2021, la société a transmis aux services de la Commission les pièces complémentaires sollicitées lors du contrôle.

15. Aux fins d'instruction de ces éléments, la présidente de la Commission a, le 19 décembre 2019, désigné Madame Valérie PEUGEOT en qualité de rapporteure sur le fondement de l'article 22 de la loi du 6 janvier 1978 modifiée.

16. À l'issue de son instruction, la rapporteure a, le 2 octobre 2020, fait notifier à la société [...] un rapport détaillant les manquements au RGPD qu'elle estimait constitués en l'espèce et indiquant à la société qu'elle disposait d'un délai d'un mois pour communiquer ses observations écrites en application des dispositions de l'article 40 du décret n° 2019-536 du 29 mai 2019.

17. Ce rapport proposait à la formation restreinte de la Commission de prononcer une injonction de mettre en conformité le traitement avec les dispositions des articles L. 34-5 du code des postes et des communications électroniques (ci-après le " CPCE "), 82 de la loi Informatique et Libertés et 5-1-e), 13, 17 et 32 du RGPD, assortie d'une astreinte par jour de retard à l'issue d'un délai de trois mois suivant la notification de la délibération de la formation restreinte, ainsi qu'une amende administrative. Il proposait également que cette décision soit rendue publique, mais qu'il ne soit plus possible d'identifier nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

18. Le 2 novembre 2020, par l'intermédiaire de son conseil, la société a produit des observations.

19. Le 5 novembre 2020, une convocation à la séance de la formation restreinte du 10 décembre 2020 a été adressée à la société.

20. Le 13 novembre 2020, la rapporteure a sollicité un délai pour répondre aux observations formulées par la société [...]. Par courriel du 16 novembre 2020, le président de la formation restreinte a avisé la rapporteure qu'elle bénéficiait d'un délai supplémentaire de huit jours pour produire ses observations. Par courrier du 24 novembre 2020, la société a été avisée qu'elle bénéficiait également d'un délai supplémentaire de huit jours et que, dès lors, la séance de la formation restreinte initialement prévue le 10 décembre 2020 était reportée.

21. Le 16 décembre 2020, la société a produit de nouvelles observations en réponse à celles de la rapporteure.

22. Par courrier daté du 11 janvier 2021, les services de la Commission ont adressé à la société une nouvelle convocation à la séance de la formation restreinte du 28 janvier 2021.

23. La société et la rapporteure ont présenté des observations orales lors de cette séance.

24. Le 19 mai 2021, dans le cadre de la procédure de coopération, un projet de décision a été soumis aux autorités concernées sur le fondement de l'article 60 du RGPD concernant les manquements au RGPD.

25. Ce projet n'a pas donné lieu à des objections pertinentes et motivées.

II. Motifs de la décision

A. Sur le manquement à l'obligation de définir et de respecter une durée de conservation des données à caractère personnel proportionnée à la finalité du traitement en application de l'article 5-1-e) du RGPD

26. Aux termes de l'article 5-1 e) du Règlement, les données à caractère personnel doivent être " conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées pour des

durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation)".

27. La rapporteure a relevé que, lors du contrôle du 13 novembre 2018, la société a indiqué à la délégation qu'aucune durée de conservation des données à caractère personnel des clients (les clients étant selon la société les détenteurs d'un compte sur le site ayant déjà effectué au moins un achat) et des prospects (détenteurs d'un compte sur le site n'ayant jamais effectué d'achat) n'avait été déterminée et qu'elle ne procédait à aucun effacement régulier ni aucun archivage de telles données à l'issue d'une période définie.

28. En défense, bien qu'elle n'en ait pas fait état lors du contrôle, la société a d'abord fait valoir qu'une politique de durée de conservation avait été définie dès le 26 octobre 2018, de telle sorte qu'aucun manquement ne pouvait lui être reproché au titre de la définition des durées de conservation.

29. Dans ses observations du 16 décembre 2020, la société a ensuite indiqué que les données des clients et prospects utilisées à des fins de prospection commerciale ou relatives à la gestion de leur compte étaient désormais conservées en base active jusqu'à la suppression du compte ou, en cas d'inactivité, pendant trois ans à compter de leur dernière connexion au compte. A l'issue de ces délais, la société a précisé que seules les données nécessaires à des finalités précontentieuses ou contentieuses sont archivées jusqu'à la date correspondant à la prescription légale justifiant leur conservation puis qu'elles seraient supprimées.

30. Enfin, lors de la séance de la formation restreinte et alors que la procédure d'instruction était close, la société a produit un document visant à apporter la preuve du déploiement d'une procédure d'archivage intermédiaire et d'un processus d'anonymisation des données. Par courriel du 10 février 2021, la société a transmis, par l'intermédiaire de son conseil, un procès-verbal réalisé le 5 février 2021, ainsi que son annexe, relatifs à la procédure d'anonymisation des données des prospects et clients de la société [...].

31. Selon la formation restreinte, s'agissant de la définition de durées de conservation applicables aux données des clients et prospects de la société [...], il y a tout d'abord lieu de relever que le document intitulé " Procédure de conservation des données à caractère personnel " est daté du 26 octobre 2018, soit antérieurement au contrôle. Il n'a pourtant été communiqué à la délégation que deux mois après la réalisation du contrôle, le 5 février 2019, et au jour du contrôle, le 13 novembre 2018, la société a indiqué à la délégation qu'" aucune durée de conservation n'est implémentée en base de données ".

32. La formation restreinte relève ensuite que lors du contrôle du 13 novembre 2018, la délégation a constaté la présence, en base active, de données à caractère personnel de 16 653 personnes n'ayant pas passé commande depuis plus de cinq ans, sans que la société soit en mesure d'avancer une explication ou d'apporter une justification quant à la durée de cette conservation ou d'apporter la preuve d'un contact plus récent avec lesdits clients (échange avec le service clients, clic sur un lien promotionnel figurant dans un courrier électronique, etc.). De plus, la formation restreinte relève qu'en réponse à une demande de compléments des services de la CNIL, la société a fourni, le 4 mars 2020, un tableau Excel dont il ressort qu'elle conservait en base les données à caractère personnel de plus de 130 000 personnes qui ne s'étaient pas connectées à leur compte client depuis plus de cinq ans.

33. Dès lors, si la formation restreinte prend note que la société [...] met désormais en œuvre des durées de conservation dont le respect permet de se conformer aux dispositions de l'article 5-1-e) du RGPD – en garantissant que les données ne sont pas conservées pour des durées excédant celle nécessaire au regard des finalités pour lesquelles elles sont traitées – elle estime, en tout état de cause, qu'au jour du contrôle, la politique de durées de conservation n'était pas respectée et que les données étaient conservées pour des durées excessives. La délégation de contrôle de la CNIL a en effet constaté que les données à caractère personnel étaient conservées pendant des durées bien plus longues que celles définies dans le document précité et qui n'apparaissaient pas adaptées au regard des finalités pour lesquelles les données sont traitées.

34. En outre, la formation restreinte considère que la société n'avait pas fourni, à la date de la clôture de l'instruction, d'éléments permettant d'attester d'une mise en conformité sur ce point. Elle considère en tout état de cause que, conformément à l'article 40 du décret du 29 mai 2019 pris pour l'application de la loi " Informatique et Libertés ", les éléments remis lors de la séance du 28 janvier 2021 ne sont pas, en l'état, suffisants pour se prononcer à ce stade sur sa mise en conformité éventuelle à l'article 5-1-e) du RGPD.

35. Au regard de l'ensemble de ces éléments, la formation restreinte considère que le manquement à l'article 5-1-e) du RGPD est caractérisé et que la société ne s'est pas complètement mise en conformité à la date de clôture de l'instruction.

B. Sur le manquement relatif à l'obligation d'informer les personnes en application de l'article 13 du RGPD

36. L'article 13 du RGPD exige du responsable de traitement qu'il fournisse, au moment où les données sont collectées, les informations relatives à son identité et ses coordonnées, celles du délégué à la protection des données, les finalités du traitement et sa base juridique, les destinataires ou les catégories de destinataires des données à caractère personnel, le cas échéant leur transferts, leur durée de conservation, les droits dont bénéficient les personnes ainsi que le droit d'introduire une réclamation auprès d'une autorité de contrôle.

37. La rapporteure relève que, tel qu'il ressort des constatations effectuées lors du contrôle sur place du 13 novembre 2018, puis du contrôle en ligne du 6 février 2020, l'information mise à disposition des utilisateurs du site n'était pas complète au sens de l'article 13 du Règlement. En effet, certaines mentions obligatoires prévues par cet article – à savoir les coordonnées du délégué à la protection des données, les durées de conservation, les bases juridiques des traitements et certains droits dont les personnes bénéficient au titre du RGPD – n'étaient pas portées à la connaissance des personnes concernées sur le site [...], que ce soit par le biais des conditions générales de vente, des " mentions légales et données personnelles " ou de la politique de conservation des données à caractère personnel.

38. En défense, la société indique avoir procédé à des rectifications, dans le cadre de la procédure, afin de délivrer une information conforme aux exigences du RGPD.

39. En premier lieu, s'agissant des coordonnées du délégué à la protection des données, la formation restreinte relève que la société a reconnu que celles-ci n'étaient pas présentes sur le site [...] jusqu'à la notification du rapport de sanction, mais a précisé qu'il était néanmoins possible de lui adresser une demande via une rubrique " désabonnement et désinscription " au sein d'un formulaire de contact.

40. Sur ce point, la formation restreinte rappelle d'abord que, bien que pouvant être une modalité utile, permettre aux clients et prospects d'être mis en relation avec le délégué à la protection des données via un formulaire de contact dédié aux " désabonnement et désinscription " n'est pas une mesure de nature à permettre le respect les dispositions de l'article 13 du RGPD, qui impose de fournir les " coordonnées " du délégué à la protection des données. De plus, la formation restreinte relève qu'à la date du contrôle sur place du 13 novembre 2018, ce formulaire était accessible depuis une rubrique intitulée " Service Client – contactez-nous " dont il est précisé qu'elle permettait de poser des " questions à propos d'une commande ou des informations sur [les] produits [de la société] ". Dans ces conditions, les personnes concernées ne pouvaient pas spontanément s'attendre à être mises en relation avec le délégué à la protection des données pour exercer leurs droits au titre du RGPD. En tout état de cause, les personnes pouvaient souhaiter utiliser les coordonnées du délégué à la protection des données pour adresser des demandes d'exercice des droits qui ne portaient pas uniquement sur des demandes de désabonnement et de désinscription, par exemple une demande de droit d'accès.

41. Dans ces conditions, la formation restreinte considère que la société n'a pas respecté les dispositions de l'article 13 du RGPD.

42. La formation restreinte relève néanmoins que la société a adopté des mesures dans le cadre de la procédure de sanction et a justifié avoir mis en conformité sa politique de protection des données qui contient à présent les coordonnées du délégué à la protection des données.

43. En deuxième lieu, s'agissant des durées de conservation, la société a indiqué avoir informé les services de la CNIL par courriel du 5 février 2019 que sa politique de conservation des données avait été mise à disposition des personnes concernées sur son site [...] à la suite du contrôle sur place du 13 novembre 2018.

44. A cet égard, la formation restreinte relève d'abord que les constats effectués lors du contrôle du 13 novembre 2018 attestent de l'absence d'information sur les durées de conservation dans les " mentions légales et données personnelles ", les " conditions générales de vente " ou tout autre document disponible sur le site internet de la société. La formation restreinte note ensuite que, si lors du contrôle en ligne du 6 février 2020, la délégation a bien constaté la présence d'un lien renvoyant vers une politique de conservation des données personnelles, cette dernière a également constaté que ce lien était inactif. Dès lors, ladite politique était inaccessible aux utilisateurs, celle-ci n'étant pas disponible par ailleurs sur le site.

45. Dans ces conditions, la formation restreinte considère que le manquement à l'article 13 du RGPD est bien constitué sur ce point dès lors que les données à caractère personnel sont collectées auprès de la personne concernée et que l'information sur les durées de conservation figure parmi celles devant être communiquées dans ce cas, en ce qu'elle permet de garantir un traitement équitable et transparent des données à caractère personnel concernées. Ainsi, par exemple, une information sur les durées de conservation permet aux personnes concernées de savoir pendant combien de temps les données sont conservées par le responsable de traitement et, par suite, pendant combien de temps elles peuvent exercer leur droit d'accès.

46. La formation restreinte relève néanmoins que, dans le cadre de la procédure de sanction, la société a justifié avoir mis en conformité sa politique de protection des données qui contient à présent les mentions relatives aux durées de conservation des données traitées.

47. En troisième lieu, s'agissant de l'information portant sur les bases légales, la société n'a pas contesté que jusqu'au 30 octobre 2020, aucune information relative aux bases légales n'était mise à disposition des personnes concernées dans le document intitulé " mentions légales et données personnelles ". Elle a cependant soutenu " qu'il ne peut lui être reproché une absence totale d'information relative aux bases juridiques dans la mesure où certaines d'entre elles étaient disponibles à travers différents supports ", par exemple dans les conditions générales de vente, et qu'un " travail de compilation était en cours au moment des contrôles ".

48. La formation restreinte relève que jusqu'au 30 octobre 2020, les personnes concernées n'étaient pas informées de l'ensemble des bases légales des traitements mis en œuvre. En tout état de cause, si certaines informations étaient disponibles dans d'autres documents, la formation restreinte relève qu'elles n'étaient pas exhaustives, et en outre que l'accessibilité et la fourniture de l'information au moment de la collecte des données de la personne concernée sont une condition exigée en application du considérant 61 et des articles 12 et 13 du RGPD.

49. Au vu de ce qui précède, la formation restreinte considère que la société ne respectait pas les dispositions de l'article 13 du RGPD.

50. La formation restreinte relève néanmoins que, au cours de la procédure de sanction, la société a justifié avoir mis en conformité sa politique de protection des données qui contient à présent une information complète portant sur les bases légales.

51. En quatrième lieu, s'agissant de l'information portant sur les droits des personnes concernées, la société a soutenu que " l'absence de mention de certains droits Informatique et libertés sur le site [...] résulte d'un simple oubli et ne constitue en aucun cas une volonté de la part de [...] d'empêcher l'exercice de certains droits par les personnes concernées ".

52. La formation restreinte relève néanmoins que, lors des vérifications effectuées le 13 novembre 2018 et le 6 février 2020, la délégation de contrôle a constaté que la société ne portait pas à la connaissance des personnes concernées leurs droits à la limitation du traitement, à la portabilité des données ainsi que celui d'introduire une réclamation auprès d'une autorité de contrôle.

53. Dans ces conditions, la formation restreinte considère que le manquement à l'article 13 du RGPD est constitué sur ce point dès lors que les données à caractère personnel sont collectées auprès de la personne concernée et que les informations manquantes en l'espèce figurent parmi celles devant être communiquées dans ce cas. En effet, l'information des personnes sur l'ensemble de leurs droits contribue à garantir un traitement équitable et transparent, en ce qu'elle facilite leur exercice et contribue ainsi à assurer la maitrise des personnes concernées sur le traitement de leurs données.

54. La formation restreinte relève néanmoins que la société a justifié avoir mis en conformité sa politique de protection des données qui contient à présent une information complète sur les droits des personnes concernées. En outre, la société indique avoir mis en ligne une page destinée à la description des droits dont les personnes bénéficient au titre du RGPD, accessible via un lien présent en pied de chaque page de son site.

55. Dès lors, la formation restreinte considère que les faits précités constituent un manquement à l'article 13 du RGPD, mais que la société s'est mise en conformité à la date de clôture de l'instruction sur l'ensemble des points soulevés.

C. Sur le manquement relatif à l'obligation de respecter la demande d'effacement des données à caractère personnel en application de l'article 17 du RGPD

56. En application de l'article 17 du RGPD, la personne concernée a le droit " d'obtenir du responsable de traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant " et le responsable de traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique :

a) les données personnelles ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;

b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a) (…) et il n'existe pas d'autre fondement juridique au traitement ;

c) la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2 (…) ".

57. Lors du contrôle du 13 novembre 2018, la délégation de contrôle a été informée que lorsqu'une personne demande l'effacement de son compte, la société ne supprime pas les données à caractère personnel mais procède uniquement à la désactivation du compte en question, empêchant la personne de s'y connecter et bloquant l'envoi de prospection commerciale. La délégation a ainsi constaté la présence en base des données à caractère personnel d'un client de la

société (nom, prénom et adresse électronique) qui avait précédemment formulé une demande d'effacement par courriel. L'accès à son compte avait été simplement désactivé.

58. La formation restreinte retient qu'il est ainsi établi que la société ne donnait pas pleinement suite aux demandes d'effacement.

59. La formation restreinte considère que si, après une demande d'effacement, certaines données à caractère personnel des clients peuvent être conservées en archivage intermédiaire, notamment au titre des obligations légales ou à des fins probatoires ou lorsque la société dispose d'un motif légitime impérieux, celles non nécessaires dans le cadre du respect de ces autres obligations ou finalités doivent être supprimées après l'exercice de ce droit dès lors que les conditions posées par l'article 17 du RGPD sont remplies. Elle relève à cet égard que tel était à tout le moins le cas pour le traitement de l'adresse électronique utilisée à des fins de prospection commerciale, dès lors que ce traitement repose sur le consentement et que le droit à l'effacement est ouvert en cas de retrait de consentement, et qu'il ne ressort pas des éléments de la procédure que la conservation des données en question était légitime sur un autre fondement.

60. Au vu de ce qui précède, la formation restreinte considère que le manquement à l'article 17 du RGPD est constitué.

61. Elle relève néanmoins que, dans le cadre de la procédure de sanction, la société a justifié avoir pris des mesures de mise en conformité avec l'article 17 du RGPD.

62. La société a d'abord justifié avoir procédé à l'effacement des données du client qui avait exercé son droit à l'effacement. Elle a ensuite précisé avoir pris différentes mesures pour améliorer le traitement des demandes d'exercice des droits, en centralisant la réception des demandes, en mettant en ligne un formulaire d'exercice des droits - téléchargeable en ligne via un lien direct inséré sur la page d'information dédiée aux droits des personnes - et en créant l'adresse électronique " dpo@[...] ", dédiée aux questions relatives aux données à caractère personnel et gérée par le délégué à la protection des données de la société. De plus, la société a indiqué avoir mis en place un document contenant des modèles de lettre de réponse aux demandes d'exercice des droits, dont un courrier de réponse aux demandes d'exercice du droit à l'effacement. En dernier lieu, la société s'est engagée à mettre en place un traçage des demandes d'exercice des droits dans un outil spécifique.

D. Sur le manquement relatif à l'obligation d'assurer la sécurité des données à caractère personnel en application de l'article 32 du RGPD

63. Aux termes de l'article 32 du RGPD " 1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre 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 œuvre 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 ;

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 […]".

64. En premier lieu, la rapporteure relève tout d'abord qu'au moment du contrôle du 13 novembre 2018, l'authentification lors de la création d'un compte sur le site [...] reposait sur un mot de passe composé uniquement de six caractères numériques, de type " 123456 ". La rapporteure relève ensuite que, s'agissant des salariés de la société, le mot de passe pour accéder au logiciel de gestion de la relation client […] était composé de huit caractères, contenant au moins un chiffre et une lettre. La rapporteure relève enfin que l'authentification des salariés aux bases de données était insuffisamment sécurisée en raison de la conservation des mots de passe permettant d'y accéder, en clair, dans un fichier texte contenu dans un ordinateur de la société.

65. En défense, la société ne conteste pas ces faits, mais soutient que l'obligation de sécurité résultant de l'article 32 du RGPD était une obligation de moyen et non de résultat, de sorte que l'obligation de sécurité du responsable du traitement consiste à mettre en œuvre les mesures permettant de réduire les risques à un niveau acceptable, sans qu'il soit obligatoire, ni même possible, d'obtenir un niveau de sécurité les rendant nuls. La société a également souligné qu'elle n'a jamais subi de violation de données à caractère personnel.

66. La formation restreinte considère que l'absence de violation de données à caractère personnel ne suffit pas à démontrer l'absence de manquement pas plus qu'une violation de données ne suffit à caractériser en soi un manquement à l'article 32 du RGPD. Il appartient à la formation restreinte de vérifier que le responsable de traitement ou, le cas échéant, le sous-traitant, a mis en œuvre, en application de cet article, des mesures techniques et organisationnelles appropriées pour prévenir les risques de violations et de mésusage de ces données. Le caractère approprié des mesures s'apprécie en vérifiant que le mis en cause a proportionné ces mesures, en l'état des informations dont il pouvait disposer par des diligences raisonnables, à la gravité et à la probabilité des risques prévisibles, en fonction de la nature et du contexte du traitement de données, ainsi que du coût et de la complexité des mesures possibles.

67. La formation restreinte considère ensuite que la longueur et la complexité d'un mot de passe demeurent des critères élémentaires permettant d'apprécier la force de celui-ci. Elle relève à cet égard que la nécessité d'un mot de passe fort est également soulignée par l'Agence nationale de sécurité des systèmes d'information.

68. À titre d'éclairage, la formation restreinte rappelle que pour assurer un niveau de sécurité suffisant et satisfaire aux exigences de robustesse des mots de passe, lorsqu'une authentification repose uniquement sur un identifiant et un mot de passe, la CNIL recommande, dans sa délibération n° 2017-012 du 19 janvier 2017, que le mot de passe comporte au minimum douze caractères - contenant au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial - ou alors comporte au moins huit caractères - contenant trois de ces quatre catégories de caractères - s'il est accompagné d'une mesure complémentaire comme, par exemple, la temporisation d'accès au compte après plusieurs échecs (suspension temporaire de l'accès dont la durée augmente à mesure des tentatives), la mise en place d'un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (comme un " captcha ") et/ou le blocage du compte après plusieurs tentatives d'authentification infructueuses.

69. En l'espèce, la formation restreinte considère qu'au regard des règles peu exigeantes encadrant leur composition, la robustesse des mots de passe admis par la société était trop faible, conduisant à un risque de compromission des comptes associés et des données à caractère personnel qu'ils contiennent.

70. Enfin, la formation restreinte rappelle que le fait de stocker les mots de passe d'accès aux bases de données en clair dans un fichier texte contenu dans un ordinateur de la société n'est pas une solution de gestion sécurisée des mots de passe. En effet, une authentification reposant sur l'utilisation d'un mot de passe court ou simple peut conduire à des attaques par des tiers non autorisés, telles que des attaques " par force brute " qui consistent à tester successivement et de façon systématique de nombreux mots de passe et permettre, ainsi, une compromission des comptes associés et des données qu'ils contiennent.

71. Dans ces conditions, la formation restreinte considère que la politique de gestion des mots de passe de la société mise en cause n'était pas suffisamment robuste et contraignante pour garantir la sécurité des données, au sens de l'article 32 du RGPD.

72. Elle relève néanmoins que, dans le cadre de la procédure de sanction, la société a indiqué, s'agissant des comptes clients, qu'elle exige désormais un mot de passe robuste comprenant un minimum de douze caractères dont une majuscule, une minuscule, un caractère numérique et un caractère spécial, ce qui a été corroboré par une impression d'écran. S'agissant des salariés, la société a mis en œuvre un mot de passe robuste pour accéder au logiciel de gestion de la relation client […]. S'agissant du stockage des mots de passe d'accès aux bases de données dans un fichier en clair, elle a justifié avoir arrêté cette pratique et mis en place une solution sécurisée de gestion des mots de passe, en souscrivant à la solution […] qui garantit un stockage chiffré des mots de passe.

73. En deuxième lieu, la rapporteure relève que la fonction de hachage utilisée pour la conservation des mots de passe des salariés utilisateurs du site [...] était obsolète (MD5).

74. En défense, la société ne conteste pas ces faits, mais reprend le même argumentaire sur l'obligation de moyen.

75. La formation restreinte rappelle que le recours à la fonction de hachage MD5 par la société n'est plus considérée depuis 2004 comme à l'état de l'art et son utilisation en cryptographie ou en sécurité est proscrite. Ainsi, l'utilisation de cet algorithme permettrait à une personne ayant connaissance du mot de passe haché de déchiffrer celui-ci sans difficulté en un temps très court (par exemple, au moyen de sites internet librement accessibles qui permettent de retrouver la valeur correspondante au hash du mot de passe).

76. Dans ces conditions, eu égard aux risques encourus par les personnes rappelés ci-dessus, la formation restreinte considère que le système de hachage utilisé ne permettait pas de garantir la sécurité des données, au sens de l'article 32 du RGPD.

77. Elle relève néanmoins que, dans le cadre de la procédure de sanction, la société a justifié avoir mis en œuvre un système de hachage satisfaisant, en SHA256, de l'ensemble des mots de passe des utilisateurs.

78. En troisième lieu, la rapporteure note que les salariés de la société accédaient à une copie de la base de production de la société [...] par un compte commun à quatre salariés.

79. En défense, la société ne conteste pas ces faits, mais reprend le même argumentaire sur l'obligation de moyen.

80. La formation restreinte rappelle que l'attribution d'un identifiant unique par utilisateur et l'interdiction des comptes partagés figurent parmi les précautions indispensables afin de garantir une traçabilité effective des accès à une base de données. En l'espèce, le partage du compte permettant d'accéder à la copie de la base de données de production par quatre salariés ne permet pas de garantir une authentification correcte des utilisateurs et, par conséquent, une gestion effective des habilitations et une traçabilité correcte des accès. Une telle absence de traçabilité des accès ne permet ainsi pas d'identifier un accès frauduleux ou l'auteur d'une éventuelle détérioration ou d'une suppression des données à caractère personnel.

81. Dans ces conditions, la formation restreinte considère que l'utilisation d'un compte générique ne permet pas de garantir la sécurité des données, au sens de l'article 32 du RGPD.

82. Elle relève néanmoins que, dans le cadre de la procédure de sanction, la société a justifié avoir pris des mesures en mettant en place un système d'authentification par utilisateur accrédité.

E. Sur le manquement aux obligations relatives aux informations (cookies) stockées sur l'équipement terminal de communications électroniques des utilisateurs en application de l'article 82 de la loi " Informatique et Libertés "

83. L'article 82 de la loi " Informatique et Libertés " impose que les utilisateurs soient informés et que leur consentement soit recueilli avant toute opération d'inscription ou d'accès à des informations déjà stockées dans leur équipement. Tout dépôt de cookies ou autres traceurs doit donc être précédé de l'information et du consentement des personnes. Cette exigence ne s'applique pas aux cookies ayant " pour finalité exclusive de permettre ou faciliter la communication par voie électronique " ou étant " strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur ".

84. La rapporteure considère que la société ne respectait pas ces dispositions dès lors qu'il ressort des contrôles en ligne des 6 février 2020 et 13 janvier 2021 qu'en arrivant sur le site web [...] plusieurs cookies ne rentrant pas dans le champ des deux exceptions rappelées ci-avant étaient déposés sur le terminal de l'utilisateur dès son arrivée sur la page d'accueil du site, et avant toute action de sa part.

85. La société ne conteste pas ces faits.

86. La formation restreinte relève en effet qu'il ressort des constatations effectuées lors du contrôle en ligne du 6 février 2020 que le dépôt de trente-deux cookies était automatique dès l'arrivée sur la page d'accueil du site, et avant tout action de l'utilisateur. En réponse à une demande de complément des services de la CNIL, la société a indiqué le 4 mars 2020 que les finalités des cookies déposés consistent à avoir " une meilleure connaissance des clients ", un " meilleur ciblage publicitaire " et à personnaliser " l'offre et des opérations promotionnelles ".

87. La formation restreinte relève également qu'alors même que la société avait affirmé, dans ses observations en réponse du 16 décembre 2020, avoir " cessé, depuis le 10 novembre 2020, de déposer des cookies soumis à consentement de manière automatique " lors de l'arrivée des utilisateurs sur son site, la délégation a constaté, lors du contrôle en ligne du 13 janvier 2021, le dépôt de treize cookies dès son arrivée sur le site. Par courriel du 26 janvier 2021, la société a transmis les pièces complémentaires sollicitées lors du contrôle et a notamment confirmé que, parmi lesdits cookies déposés, certains avaient une finalité publicitaire.

88. Dès lors, les cookies déposés n'ayant pas pour finalité exclusive de permettre ou de faciliter la communication par voie électronique et n'étant pas strictement nécessaires à la fourniture du service, leur dépôt imposait à la société de recueillir préalablement le consentement des utilisateurs.

89. La formation restreinte considère, en conséquence, qu'un manquement à l'article 82 de la loi " Informatique et Libertés " est constitué.

90. La formation restreinte souligne néanmoins que la société a apporté d'importantes modifications sur son site web durant la procédure de sanction et que les cookies pour lesquels le consentement des utilisateurs est requis ne sont plus déposés automatiquement dans le terminal de l'utilisateur à l'arrivée sur la page d'accueil du site depuis le 26 janvier 2021.

F. Sur le manquement relatif à l'obligation de recueillir le consentement de la personne concernée par une opération de prospection directe au moyen d'un courrier électronique en application de l'article L. 34-5 du CPCE

91. Aux termes de l'article L. 34-5 du CPCE : " Est interdite la prospection directe au moyen de système automatisé de communications électroniques au sens du 6° de l'article L. 32, d'un télécopieur ou de courriers électroniques utilisant les coordonnées d'une personne physique, abonné ou utilisateur, qui n'a pas exprimé préalablement son consentement à recevoir des prospections directes par ce moyen.

Pour l'application du présent article, on entend par consentement toute manifestation de volonté libre, spécifique et informée par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées à fin de prospection directe. […]

Toutefois, la prospection directe par courrier électronique est autorisée si les coordonnées du destinataire ont été recueillies auprès de lui, dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, à l'occasion d'une vente ou d'une prestation de services, si la prospection directe concerne des produits ou services analogues fournis par la même personne physique ou morale, et si le destinataire se voit offrir, de manière expresse et dénuée d'ambiguïté, la possibilité de s'opposer, sans frais, hormis ceux liés à la transmission du refus, et de manière simple, à l'utilisation de ses coordonnées au moment où elles sont recueillies et chaque fois qu'un courrier électronique de prospection lui est adressé au cas où il n'aurait pas refusé d'emblée une telle exploitation ".

92. La rapporteure relève qu'à l'occasion des contrôles effectués les 13 novembre 2018 et 6 février 2020, la délégation a constaté que, lors de la création d'un compte sans acte d'achat sur le site web de la société, aucun procédé visant à recueillir le consentement à la collecte et au traitement des données à caractère personnel à des fins de prospection commerciale par courriers électroniques n'était mis en œuvre.

93. En défense, la société soutient qu'en raison des mentions d'information présentes sur le site, les personnes ayant créé un compte ne pouvaient ignorer que la société leur adresserait de manière régulière des communications commerciales par courrier électronique. Elle rappelle également que pour valider une inscription lors de la création d'un compte sur le site de la société, la personne doit accepter les conditions générales de vente de la société qui prévoient que ses données à caractère personnel seront utilisées par la société afin de l'informer par courriers électroniques des ventes à venir et des offres spéciales.

94. La formation restreinte considère que la création d'un compte ne préjuge pas de la commande éventuelle de produits auprès de la société [...]. La formation restreinte considère qu'en l'absence d'achat, la société ne peut utilement invoquer le bénéfice de l'exception créée par l'article L. 34-5 du CPCE permettant la prospection sans consentement préalable lorsque les coordonnées du destinataire ont été recueillies auprès de lui à l'occasion d'une vente ou d'une prestation de services si la prospection directe concerne des produits ou services analogues fournis par la même personne physique ou morale.

95. Dès lors, la formation restreinte considère qu'il appartenait à la société de recueillir le consentement préalable, libre, spécifique et informé des personnes créant un compte sur le site web de la société sans avoir procédé à un achat, à recevoir des messages de prospection directe par courriers électroniques, conformément à l'alinéa 1 de l'article L. 34-5 du CPCE.

96. Dans ces conditions, la formation restreinte considère que le manquement à l'article L. 34-5 du CPCE est constitué.

Dans le cadre de la procédure, la société a justifié avoir inséré sur le formulaire de création de compte en ligne une case à cocher permettant la prise en compte d'un consentement spécifique et univoque pour les personnes souhaitant créer à l'avenir un compte.

97. Pour les personnes qui étaient déjà titulaires d'un compte sur le site [...], la société indique qu'elle envisage d'adresser des courriers électroniques de prospection aux seules personnes ayant déjà effectué un achat sur son site. Elle indique en outre avoir adressé des courriels afin d'obtenir l'accord de […] prospects n'ayant pas encore donné leur consentement à recevoir de la prospection par voie électronique ni effectué d'achat à la suite de la création de leur compte.

98. Lors de la séance de la formation restreinte, la société a en outre précisé qu'afin de se mettre en conformité avec les dispositions de l'article L. 34-5 du CPCE, elle comptait adresser à chaque prospect n'ayant pas encore donné son consentement cinq courriels visant à obtenir leur accord à recevoir de la prospection par voie électronique. Ces cinq courriels seraient envoyés au cours d'une période de 100 jours à compter de la date de dernière activité du prospect. La société a indiqué qu'au bout de 100 jours d'inactivité de la part du prospect et sans consentement de ce dernier à recevoir de la prospection commerciale à la suite des cinq courriels qu'elle lui aura adressés, elle cessera de le prospecter.

99. La formation restreinte considère que le fait de solliciter les personnes en question pour leur demander si elles souhaitent recevoir des courriels de prospection constitue en soi un traitement qui ne saurait reposer, en l'espèce, que sur un éventuel intérêt légitime de la société. Il résulte des pièces du dossier que les prospects, en choisissant de créer un compte sur le site de la société pour avoir accès à ses offres, ont manifesté un certain intérêt pour les services proposés par cette dernière et que, dès lors, ils peuvent raisonnablement s'attendre à ce que la société les contacte. Elle considère

cependant que l'envoi aux prospects de cinq courriels, a fortiori au cours d'une période de 100 jours, excède le nombre de courriels auxquels pourraient raisonnablement s'attendre ces derniers.

100. Dans ces conditions, la formation restreinte considère que la société ne s'est pas complètement mise en conformité à la date de clôture de l'instruction.

III. Sur les mesures correctrices et leur publicité

101. Aux termes du III de l'article 20 de la loi du 6 janvier 1978 modifiée :

" Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut également, le cas échéant après lui avoir adressé l'avertissement prévu au I du présent article ou, le cas échéant en complément d'une mise en demeure prévue au II, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes : […]

2° Une injonction de mettre en conformité le traitement avec les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie, sauf dans des cas où le traitement est mis en œuvre par l'État, d'une astreinte dont le montant ne peut excéder 100 000 € par jour de retard à compter de la date fixée par la formation restreinte ; […]

7° À l'exception des cas où le traitement est mis en œuvre par l'État, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du règlement (UE) 2016/679 du 27 avril 2016, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83. "

L'article 83 du RGPD prévoit que " Chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives ", avant de préciser les éléments devant être pris en compte pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de cette amende.

102. En premier lieu, sur le principe du prononcé d'une amende, la société soutient qu'une telle mesure n'est pas justifiée. Elle souligne notamment qu'elle n'a jamais été condamnée par la formation restreinte, que les manquements précités ne constituent en aucun cas une violation délibérée du RGPD, que les personnes concernées n'ont pas subi de dommage, qu'aucune donnée particulière visée aux articles 9 et 10 du RGPD n'est concernée, qu'elle a coopéré de bonne foi avec la CNIL tout au long de la procédure et qu'elle a pris des mesures de mise en conformité.

103. La formation restreinte rappelle qu'elle doit tenir compte, pour le prononcé d'une amende administrative, des critères précisés à l'article 83 du RGPD, tels que la nature, la gravité et la durée de la violation, les mesures prises par le responsable du traitement pour atténuer le dommage subi par les personnes concernées, le degré de coopération avec l'autorité de contrôle et les catégories de données à caractère personnel concernées par la violation.

104. La formation restreinte considère d'abord que la société a fait preuve de négligence grave s'agissant de principes fondamentaux du RGPD puisque six manquements sont constitués, portant notamment sur le principe de limitation de la durée de conservation des données, l'obligation d'informer les personnes concernées des traitements de leurs données à caractère personnel et celle de respecter leurs droits.

105. La formation restreinte relève ensuite que plusieurs manquements constatés ont concerné un nombre important de personnes, à savoir […] utilisateurs en France, […] en Espagne, […] en Italie et […] au Portugal.

106. Enfin, la formation restreinte relève que les mesures de mise en conformité mises en place à la suite de la notification du rapport de sanction ne concernent pas tous les manquements et n'exonèrent pas la société de sa responsabilité pour le passé, notamment au vu des manquements constatés.,

107. En conséquence, la formation restreinte considère qu'il y a lieu de prononcer une amende administrative au regard des manquements aux articles 5-1-e), 13, 17 et 32 du RGPD, 82 de la loi " Informatique et Libertés " et L. 34-5 du CPCE.

108. En deuxième lieu, s'agissant du montant de l'amende concernant les manquements au RGPD, la formation restreinte rappelle que le paragraphe 3 de l'article 83 du Règlement prévoit qu'en cas de violations multiples, comme c'est le cas en l'espèce, le montant total de l'amende ne peut excéder le montant fixé pour la violation la plus grave. Dans la mesure où il est reproché à la société un manquement aux articles 5-1-e), 13, 17 et 32 du Règlement, 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.

109. S'agissant du montant de l'amende relative au manquement à l'article 82 de la loi " Informatique et Libertés " et à l'article L.34-5 du CPCE, la formation restreinte rappelle qu'en ce qui concerne les manquements à des dispositions trouvant leur origine dans d'autres textes que le RGPD, comme c'est le cas de l'article L.34-5 du CPCE qui transpose en droit interne la directive " ePrivacy ", l'article 20 paragraphe III de la loi " Informatique et Libertés " lui donne compétence pour prononcer diverses sanctions, notamment une amende administrative dont le montant maximal peut être équivalant à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent réalisé par le responsable de traitement. En outre, la détermination du montant de cette amende s'apprécie également au regard des critères précisés par l'article 83 du RGPD.

110. La formation restreinte rappelle également que les amendes administratives doivent être dissuasives mais proportionnées. Elle considère en particulier que l'activité de la société et sa situation financière doivent être prises en compte pour la détermination de la sanction et notamment, en cas d'amende administrative, de son montant. Elle relève à ce titre que la société fait état d'un chiffre d'affaires de 2018 à 2020 s'établissant à environ […] euros puis à environ […] euros et enfin à environ […] euros pour un résultat net respectivement de […] euros, puis de […] euros et enfin de […] euros. Elle en déduit que le montant de l'amende proposé par la rapporteure est loin d'atteindre le montant maximal de la sanction pécuniaire prévu par le RGPD puisqu'il représente au maximum […] % du chiffre d'affaires de la société. Au vu de ces éléments, la formation restreinte considère que le prononcé d'une amende de 500 000 euros apparaît justifié, soit 300 000 euros pour les manquements aux articles 5-1-e), 13, 17 et 32 du RGPD et 200 000 euros pour les manquements à l'article 82 de la loi " Informatique et Libertés " et l'article L. 34-5 du CPCE.

111. En troisième lieu, une injonction de mettre en conformité le traitement avec les dispositions des articles 5-1-e) du RGPD et L. 34-5 du CPCE a été proposée par la rapporteure lors de la notification du rapport.

112. La société soutient que les actions qu'elle a mises en œuvre s'agissant de l'ensemble des manquements relevés doivent conduire à ne pas donner suite à la proposition d'injonctions de la rapporteure.

113. S'agissant du manquement à l'obligation de définir et de respecter une durée de conservation des données à caractère personnel proportionnée à la finalité du traitement en application de l'article 5-1-e) du RGPD, la société indique avoir mis en place une procédure interne permettant d'archiver puis d'anonymiser les données.

114. La formation restreinte considère cependant que la société n'avait pas fourni, à la date de la clôture de l'instruction, d'éléments lui permettant d'attester d'une mise en conformité sur ce point. Elle considère en tout état de cause que les éléments produits lors de la séance ne sont pas suffisants pour se prononcer à ce stade sur sa mise en conformité éventuelle à l'article 5-1-e) du RGPD.

115. S'agissant du manquement relatif à l'obligation de recueillir le consentement de la personne concernée par une opération de prospection directe au moyen d'un système automatisé de communications électroniques en application de l'article L. 34-5 du CPCE, la formation restreinte considère que la société a pris les mesures satisfaisantes pour recueillir à présent le consentement des personnes lors de la création d'un compte sur le site web [...]. La formation restreinte relève également que la société s'est engagée, dans le cadre de la procédure, à ne plus procéder à l'envoi de messages de prospection directe par courriers électroniques à des prospects sans leur consentement préalable. Elle considère cependant qu'elle n'a pas démontré sa conformité complète à l'article L. 34-5 du CPCE dans la mesure où elle entend solliciter l'accord des personnes ayant créé un compte par le passé jusqu'à cinq reprises. En conséquence, la formation restreinte considère qu'il y a lieu de prononcer une injonction sur ce point.

116. En quatrième lieu, la formation restreinte considère que la publicité de la sanction se justifie au regard de la pluralité des manquements relevés, de leur persistance, de leur gravité et du nombre de personnes concernées.

PAR CES MOTIFS

La formation restreinte de la CNIL, après en avoir délibéré, décide de :

• prononcer à l'encontre de la société [...] une amende administrative d'un montant de 500 000 (cinq cent mille) euros, qui se décompose comme suit :

o 300 000 (trois cent mille) euros pour les manquements aux articles 5-1-e), 13, 17 et 32 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après " le RGPD ") ;

o 200 000 (deux cent mille) euros pour les manquements à l'article 82 de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée et à l'article L. 34-5 du code des postes et des communications électroniques (ci-après le " CPCE ") ;

• prononcer à l'encontre de la société [...] une injonction de mettre en conformité les traitements avec les obligations résultant des articles et 5-1-e) du RGPD et L. 34-5 du CPCE, et en particulier :

o s'agissant du manquement au principe de limitation de la durée de conservation des données à caractère personnel, mettre en œuvre une politique de durée de conservation des données à caractère personnel qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées, et notamment :

 cesser de conserver les données à caractère personnel des anciens clients du site web de la société à l'issue de la période d'inactivité fixée, procéder à la purge de telles données conservées par la société jusqu'à la date de la délibération de la formation restreinte et justifier de la suppression de ces données à caractère personnel au-delà d'une période d'inactivité définie, dont il appartiendra à la société de justifier ;

 justifier d'une procédure d'archivage intermédiaire des données à caractère personnel des clients, mise en place après avoir opéré un tri des données pertinentes à archiver et une suppression des données non pertinentes, ainsi que du point de départ de cet archivage (par exemple, s'agissant des factures archivées à des fins comptables) ;

o s'agissant du manquement à l'obligation de recueillir le consentement de la personne concernée par une opération de prospection directe au moyen d'un système automatisé de communications électroniques : cesser de prospecter les personnes non clientes n'ayant pas exprimé leur consentement, sauf à obtenir leur consentement ;

• assortir l'injonction d'une astreinte de 500 (cinq cents) euros par jour de retard à l'issue d'un délai de trois mois suivant la notification de la présente délibération, les justificatifs de la mise en conformité devant être adressés à la formation restreinte dans ce délai ;

• rendre publique, sur le site de la CNIL et sur le site de Légifrance, sa délibération, qui n'identifiera plus nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

Le président

Alexandre LINDEN