Délibération SAN-2024-002 du 31 janvier 2024

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Sanction
Etat juridique : En vigueur

Date de publication sur Légifrance : Mardi 13 février 2024

Délibération de la formation restreinte n°SAN-2024-002 du 31 janvier 2024 concernant la société DE PARTICULIER A PARTICULIER – EDITIONS NERESSIS

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Alexandre LINDEN, président, M. Philippe-Pierre CABOURDIN, vice-président, Mme Christine MAUGÜÉ, MM. Alain DRU et 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 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 n° 2019-536 du 29 mai 2019 modifié 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° 2021-193C du 29 juin 2021 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 de données à caractère personnel mis en œuvre par la société ou pour son compte ;

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 6 février 2023 ;

Vu le rapport de Mme Sophie LAMBREMON, commissaire rapporteur, notifié à la société DE PARTICULIER A PARTICULIER – EDITIONS NERESSIS le 20 juillet 2023 ;

Vu les observations écrites versées par la société DE PARTICULIER A PARTICULIER – EDITIONS NERESSIS le 8 septembre 2023 ;

Vu les observations en réponse de la rapporteure le 6 octobre 2023 ;

Vu les observations en réponse de la société DE PARTICULIER A PARTICULIER – EDITIONS NERESSIS le 2 novembre 2023 ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 21 décembre 2023 :

- Mme Sophie LAMBREMON, commissaire, entendue en son rapport ;

En qualité de représentants de la société DE PARTICULIER A PARTICULIER – EDITIONS NERESSIS :

- […];

La société DE PARTICULIER A PARTICULIER – EDITIONS NERESSIS ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. La société DE PARTICULIER A PARTICULIER – EDITIONS NERESSIS (ci-après " la société "), dont le siège social est situé 45 rue du Cardinal Lemoine à Paris (75005), a été immatriculée au registre du commerce et des sociétés le 14 novembre 1975. Son chiffre d'affaires s'est élevé en 2021, à […] euros pour un résultat net de […] euros et en 2022, à […] euros pour un résultat net de […] euros.

2. La société DE PARTICULIER A PARTICULIER – EDITIONS NERESSIS met à disposition des particuliers un ensemble de publications et services leur permettant de conclure des transactions immobilières sans intermédiaire. La société édite le site web www.pap.fr lequel propose aux particuliers de publier ou de consulter des annonces immobilières et d'avoir accès à différents outils permettant la gestion de projets immobiliers (assistance juridique, coaching immobilier, calculs de crédit, du prix au mètre carré, de l'évaluation du prix des biens à vendre et des frais de notaire).

3. Deux missions de contrôle ont eu lieu en application de la décision n° 2022-041C du 2 mars 2022 de la présidente de la CNIL afin de vérifier le respect par la société de l'ensemble des dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après " le RGPD " ou " le Règlement ") et de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée (ci-après " la loi Informatique et Libertés "). Le 8 mars 2022, les services de la CNIL ont effectué un contrôle en ligne à partir du site web " www.pap.fr ". Le 7 avril 2022, les services de la CNIL ont procédé à un contrôle sur place dans les locaux de la société situés à Paris (75005).

4. Le contrôle en ligne du site web www.pap.fr avait principalement pour objet de vérifier les modalités d'information des personnes et la procédure de création d'un compte utilisateur. Le contrôle sur place a plus spécifiquement porté sur la vérification des durées de conservation appliquées aux données des comptes utilisateurs, l'encadrement par un acte juridique des traitements effectués par un sous-traitant, les mesures techniques et organisationnelles destinées à assurer la sécurité des données collectées au moyen du site web ainsi que sur l'information des personnes de la prospection pour produits et services analogues.

5. Par courriels des 10 avril et 7 juin 2022, la société a transmis aux services de la Commission des éléments complémentaires.

6. Conformément à l'article 56 du RGPD, la CNIL a informé le 17 janvier 2023 l'ensemble des autorités de contrôle européennes de sa compétence pour agir en tant qu'autorité de contrôle cheffe de file concernant les traitements transfrontaliers mis en œuvre par la société, résultant de ce que l'établissement unique de la société se trouve en France. Après échanges entre la CNIL et les autorités de protection des données européennes dans le cadre du mécanisme de guichet unique, il apparaît que les autorités allemande, autrichienne, belge, danoise, espagnole, finlandaise, grecque, irlandaise, italienne, néerlandaise, norvégienne, polonaise, portugaise et suédoise sont concernées par le traitement, des comptes utilisateurs ayant été créés par des personnes résidant dans ces États.

7. Aux fins d'instruction de ces éléments, la présidente de la Commission a, le 6 février 2023, désigné Mme Sophie LAMBREMON en qualité de rapporteur sur le fondement de l'article 22 de la loi Informatique et Libertés.

8. Le 20 juillet 2023, la rapporteure a fait notifier à la société un rapport détaillant les manquements aux articles 5-1-e), 12, 13, 28 et 32 du RGPD ainsi qu'à l'article L.34-5 du code des postes et des communications électroniques, qu'elle estimait constitués en l'espèce.

9. Le 8 septembre 2023, la société a produit des observations en réponse au rapport de sanction.

10. Le 6 octobre 2023, la rapporteure a répondu aux observations de la société.

11. Le 3 novembre 2023, la société a transmis de nouvelles observations en réponse aux observations de la rapporteure.

12. Par courrier du 9 novembre 2023, la rapporteure a informé la société que l'instruction était close, en application de l'article 40, III, du décret modifié n° 2019-536 du 29 mai 2019.

13. Par courrier du même jour, la société a été informée que le dossier était inscrit à l'ordre du jour de la formation restreinte du 30 novembre 2023.

14. Par courriel du 14 novembre 2023, le conseil de la société a sollicité un renvoi de la séance de la formation restreinte.

15. Par courrier du 16 novembre 2023, le conseil de la société a été informé du report de la séance au 21 décembre 2023.

16. La rapporteure et la société ont présenté des observations orales lors de la séance de la formation restreinte.

II. Motifs de la décision

A. Sur la procédure de coopération européenne

17. En application de l'article 60 paragraphe 3 du RGPD, le projet de décision adopté par la formation restreinte a été transmis le 29 décembre 2023 aux autorités de contrôle européennes concernées.

18. Au 26 janvier 2024, aucune des autorités de contrôle concernées n'avait formulé d'objection pertinente et motivée à l'égard de ce projet de décision, de sorte que, en application de l'article 60, paragraphe 6, du RGPD, ces dernières sont réputées l'avoir approuvé.

B. Sur le manquement à l'obligation de limitation de la durée de conservation des données

19. Aux termes de l'article 5-1, e) du RGPD, 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 ".

20. La rapporteure a relevé que, lors du contrôle sur place, la société a indiqué avoir défini une politique de conservation des données différente selon le type d'usagers du site web www.pap.fr. Ainsi, concernant les données des clients (personnes ayant recours aux services payants du site), la rapporteure a relevé que la société avait défini une durée de conservation de dix ans à compter de la date d'acceptation de la commande. Elle a relevé que la conservation systématique et sans distinction de toutes les données de comptes durant dix ans n'apparaissait pas justifiée au regard de l'obligation légale tirée du code de la consommation et que dans l'extraction de la base de données fournie figuraient des données relatives à des transactions inférieures à 120 euros dont la conservation n'apparaissait pas justifiée. Concernant les données des utilisateurs (personnes ayant recours aux services gratuits du site), la rapporteure a relevé que si la société avait défini une durée de conservation de cinq ans à partir de la date de la dernière connexion au compte, il ressortait du contrôle sur place que la société avait conservé 2 394 538 lignes depuis plus de cinq ans et moins de dix ans et 737 563 lignes depuis plus de dix ans.

21. En défense, concernant les données des clients ayant recours à des annonces payantes, la société a, lors de l'instruction, précisé conserver l'annonce et l'adresse électronique durant dix ans à des fins de respect des obligations légales tirées des articles L.213-1, D.213-1 et D.213-2 du code de la consommation, de lutte contre la fraude et en raison des spécificités liées à l'activité immobilière. Elle a détaillé les deux formules payantes proposées aux clients : soit un contrat sans engagement pour 59 euros par mois qui s'analyse en un contrat unique à durée indéterminée, soit un contrat de trois mois souscrit pour 135 euros. Pour les contrats sans engagement, estimant ne pas être mesure de déterminer à l'avance la durée du contrat, la société a précisé conserver toutes les données relatives à ces contrats pour une durée de dix ans quel qu'en soit le montant final. Elle considère en outre qu'il y a lieu de prendre en compte les enjeux financiers des annonces et contrats de vente de biens conclus ensuite d'un montant bien supérieur à 120 euros. Elle a également indiqué que la durée de conservation des années de naissance était réduite à vingt-cinq mois et celle des données relatives à un compte inactif à trois ans d'inactivité.

22. Concernant les données relatives aux utilisateurs, la société a, lors de l'instruction, précisé conserver uniquement l'adresse électronique et le compte associé pour une durée de cinq ans à des fins contentieuses et de lutte contre la fraude et avoir supprimé les données conservées au-delà de cette durée de cinq ans.

23. La formation restreinte rappelle qu'il incombe au responsable de traitement de définir et de mettre en œuvre une durée de conservation des données n'excédant pas celle nécessaire au regard de la finalité pour laquelle elles sont traitées.

24. S'agissant des durées pertinentes, à titre illustratif, la formation restreinte relève que dans son référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion des activités commerciales, la CNIL précise que les données nécessaires à l'exécution d'un contrat sont conservées durant la relation contractuelle et que le respect d'une obligation légale incombant à l'organisme peut, notamment, justifier une durée de conservation plus longue. A défaut, la conservation doit reposer sur une autre base légale prévue à l'article 6 du RGPD.

25. Aux termes de l'article L. 213-1 du code de la consommation : " Lorsque le contrat est conclu par voie électronique et qu'il porte sur une somme égale ou supérieure à un montant fixé par décret, le contractant professionnel assure la conservation de l'écrit qui le constate pendant un délai déterminé par ce même décret et en garantit à tout moment l'accès à son cocontractant si celui-ci en fait la demande. ".

26. L'article D. 213-1 du même code prévoit que " [l]e montant mentionné à l'article L. 213-1 est fixé à 120 euros " et l'article D. 213-2 dispose que " [l]e délai mentionné à l'article L. 213-1 est fixé à dix ans à compter de la conclusion du contrat lorsque la livraison du bien ou l'exécution de la prestation est immédiate. Dans le cas contraire, le délai court à compter de

la conclusion du contrat jusqu'à la date de livraison du bien ou de l'exécution de la prestation et pendant une durée de dix ans à compter de celle-ci ".

27. En l'espèce, la formation restreinte relève tout d'abord, s'agissant de la conservation des données des clients, que la durée de conservation de dix ans à compter de la date d'acceptation de la commande définie par la société est justifiée par ses obligations légales résultant du code de consommation précitées pour les contrats d'un montant supérieur à 120 euros. Ainsi, la formation restreinte considère que, pour les contrats de trois mois proposés par la société d'un montant de 135 euros, la conservation des données pour une durée de dix ans est pleinement justifiée.

28. En revanche, la formation restreinte relève que, pour les contrats sans engagement d'un montant de 59 euros par mois, la société conserve par défaut les données relatives à ces contrats dès qu'ils sont conclus et quand bien même le montant total versé par l'utilisateur serait inférieur à 120 euros. Or, dans le cas où un client n'aurait utilisé les services payants de la société que pour un ou deux mois, c'est-à-dire pour une somme inférieure à 120 euros, la durée de conservation des données prévue par le code de la consommation ne trouverait pas à s'appliquer. La formation restreinte relève que l'article D.213-1 du code de la consommation précise expressément " lorsque le contrat (…) porte sur une somme égale ou supérieure ". La seule somme à prendre en considération est donc celle du contrat conclu entre la société PAP et le client, d'autant que la société PAP est tiers au contrat de vente de bien conclu entre le client vendeur et l'acheteur. Par suite, la formation restreinte considère que la conservation des données des clients se trouvant dans la situation qui vient d'être décrite n'est pas rendue obligatoire par le respect du code de la consommation, contrairement à ce que la société indique.

29. En tout état de cause, la formation restreinte constate qu'il ressort d'une extraction de 100 lignes correspondant à des comptes de clients ayant passé des commandes il y a plus de cinq ans que 69 d'entre elles concernaient des commandes d'un montant inférieur à 120 euros. Partant, la formation restreinte considère que la société a conservé les données de comptes non concernées par l'article D. 213-1 du code de la consommation pour des durées excessives.

30. Ensuite, la formation restreinte relève, s'agissant de la conservation des données des utilisateurs, que la société a défini une durée de cinq ans qui commence à courir à la date de la dernière connexion au compte utilisateur. La formation restreinte considère que les explications fournies par la société lors de l'instruction justifient la durée de conservation à des fins contentieuses et de lutte contre la fraude.

31. Néanmoins, la formation restreinte observe qu'il ressort du contrôle sur place que la société avait conservé 2 394 538 lignes correspondant à des comptes d'utilisateurs de plus de cinq ans à compter de la date de la dernière connexion et moins de dix ans et 737 563 lignes correspondant à des comptes utilisateurs de plus de dix ans à compter de la date de la dernière connexion.

32. La formation restreinte relève qu'il résulte de ce qui précède que lorsque la durée de conservation est atteinte, les données personnelles doivent être supprimées. Dès lors, il ressort des pièces du dossier qu'à la date du contrôle sur place, la société conservait les données de comptes utilisateurs au-delà de ce qui était nécessaire au regard de la finalité annoncée.

33. En conséquence, la formation restreinte considère que les faits qui précèdent caractérisent un manquement à l'article 5-1-e) du RGPD. La formation restreinte relève que la société s'est partiellement mise en conformité au cours de la procédure avec l'application d'une durée de conservation adéquate des données de comptes utilisateurs au regard des différentes finalités poursuivies en procédant à la suppression des données relatives à ces comptes inactifs depuis plus de cinq ans. Cette mise en conformité ne saurait exonérer la société de sa responsabilité pour le passé.

C. Sur le manquement à l'obligation d'information des personnes

34. L'article 13 du RGPD dresse la liste des informations devant être fournies à la personne concernée lorsque les données à caractère personnel sont collectées directement auprès d'elle. Ces informations portent notamment sur l'identité du responsable de traitement et ses coordonnées, les finalités du traitement mis en œuvre, sa base juridique, les destinataires ou les catégories de destinataires des données, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données vers un pays tiers. L'article impose également au responsable de traitement, lorsque cela apparaît nécessaire pour garantir "un traitement équitable et transparent " des données personnelles en l'espèce, d'informer les personnes sur la durée de conservation des données, l'existence des différents droits dont bénéficient les personnes, l'existence du droit de retirer son consentement à tout moment et le droit d'introduire une réclamation auprès d'une autorité de contrôle.

35. Dans son rapport, la rapporteure relève en substance que l'information fournie par la société sur le site web www.pap.fr, à travers sa page " politique de protection des données personnelles ", était incomplète ou imprécise, faute de préciser les traitements auxquels se rapportent les bases légales, les destinataires ou catégories de destinataires de données, le droit d'introduire une réclamation auprès de la CNIL et les durées de conservation définies par la société. La rapporteure note toutefois que la société s'est, depuis les contrôles, engagée dans une démarche de mise en conformité, sans que cela remette en cause les manquements pour le passé.

36. En défense, la société conteste le manquement. Elle estime seulement avoir délivré les informations de façon imprécise. Elle indique s'être mise en conformité depuis les contrôles en modifiant et complétant sa politique de protection des données personnelles. S'agissant des bases juridiques applicables aux traitements, la société évoque une maladresse de présentation. S'agissant de la mention des destinataires ou catégories de destinataires, elle considère qu'elle n'était pas tenue de fournir l'identité de l'intégralité des destinataires de données.

37. La formation restreinte relève qu'il ressort des constats faits lors des contrôles que s'agissant du site web www.pap.fr, une politique de protection des données personnelles était accessible depuis le pied de la page d'accueil, document auquel le formulaire de création d'un compte utilisateur renvoyait également. Or, il apparaît que si les bases juridiques étaient indiquées, aucune explication ne figurait s'agissant des traitements auxquels elles se rapportaient.

38. En outre, la formation restreinte relève, à l'instar de la rapporteure, que la société indiquait le nom d'un seul de ses sous-traitants, la société […], qui est en charge des paiements effectués sur le site. Hormis ce cas de figure, aucune information n'était délivrée concernant les autres destinataires ou catégories de destinataires des données à caractère personnel. Or, la formation restreinte relève qu'il ressort des contrôles que la société avait au moins deux autres sous-traitants destinataires des données à caractère personnel.

39. Aussi, la formation restreinte considère que la société n'a pas respecté les dispositions de l'article 13 (1) du RGPD.

40. Ensuite, la formation restreinte relève, d'une part, que cette politique de protection des données personnelles ne mentionnait pas le droit d'introduire une réclamation auprès de la CNIL et, d'autre part, que les durées de conservation indiquées étaient inexactes.

41. Or, la formation restreinte considère que ces informations, en ce qu'elles contribuent à assurer pour les utilisateurs la maîtrise sur le traitement de leurs données, sont importantes pour garantir un traitement équitable et transparent.

42. La formation restreinte considère que l'absence de mention du droit d'introduire une réclamation auprès de la CNIL et l'imprécision de l'information relative à la durée de conservation des données des utilisateurs dans la politique de confidentialité de la société, constituent un manquement à l'article 13 (2) du RGPD.

43. En conséquence, la formation restreinte considère que la société a commis un manquement à l'article 13 du RGPD. Elle précise que le manquement pris en compte est celui qui a été cristallisé au moment des contrôles et prend acte de ce que la société s'est mise en conformité.

D. Sur le manquement lié à l'obligation d'encadrer par un acte juridique les traitements effectués pour le compte du responsable de traitement

44. En vertu de l'article 28, paragraphe 3, du Règlement, le traitement effectué par un sous-traitant pour le compte d'un responsable de traitement est régi par un contrat ou tout autre acte juridique formalisé qui définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel, les catégories de personnes concernées ainsi que les obligations et les droits du responsable de traitement. Ce contrat prévoit en outre les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement.

45. La rapporteure a constaté que les documents contractuels des sociétés […], sous-traitantes de la société, ne contenaient pas toutes les mentions prévues par l'article susmentionné.

46. En défense, la société conteste le manquement pour ce qui concerne la relation contractuelle avec la société […]. A cet égard, elle précise que cette dernière est régie par un contrat qui renvoie à un accord de traitements des données, lequel contient les mentions exigées par l'article 28. Concernant le contrat conclu avec la société […], la société indique avoir conclu un avenant au contrat contenant les mentions prévues à l'article 28. Enfin, la société déclare avoir mis fin à la relation contractuelle avec la société […].

47. La formation restreinte relève que s'agissant des documents contractuels de la société […], la société avait fourni à la délégation de la CNIL le seul contrat conclu le 19 novembre 2021. Elle a, par la suite, versé en réponse au rapport de sanction l'accord de traitement de données auquel renvoie le contrat. La formation restreinte considère que ces documents contractuels lus dans leur ensemble comportent toutes les mentions nécessaires. Le manquement n'est donc pas constitué pour cette relation contractuelle.

48. S'agissant ensuite du contrat conclu avec la société […], la formation restreinte relève que l'avenant produit par la société en réponse au rapport de sanction a été conclu le 7 septembre 2023. La formation restreinte relève que cet avenant contient l'ensemble des mentions requises mais considère que le manquement est constitué pour le passé au regard de la date de signature dudit avenant. La formation restreinte considère en effet que le caractère rétroactif de l'avenant dont se

prévaut la société ne saurait venir couvrir le manquement pour le passé dans la mesure où lors des contrôles le contrat conclu ne contenait pas les mentions requises.

49. S'agissant enfin du contrat conclu avec la société […], la formation restreinte considère qu'eu égard aux pièces produites, il n'est pas établi que cette société traitait de données à caractère personnel pour le compte de la société PAP et disposait de la qualité de sous-traitant au sens du RGPD. Aussi le manquement à l'article 28 n'est pas caractérisé.

50. En définitive, la formation restreinte considère que le manquement à l'article 28, paragraphe 3, du RGPD est constitué pour les faits passés concernant le contrat régissant la relation avec la société […].

E. Sur les manquements à l'obligation d'assurer la sécurité des données

51. 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 ".

1. Sur les mots de passe et références confidentielles

52. La rapporteure relève que, d'une part, lors du contrôle en ligne, la délégation avait constaté que lors de la création d'un compte utilisateur sur le site web de la société, les mots de passe d'un caractère unique (un chiffre ou une lettre) étaient acceptés et qu'aucune restriction d'accès en cas d'échec d'authentification n'était mise en œuvre. En outre, la rapporteure relève que, lors des contrôles, chaque mot de passe était à la fois stocké en clair et haché avec l'algorithme de hachage Bcrypt.

53. D'autre part, la rapporteure relève que, lors du contrôle sur place, la délégation était informée qu'au dépôt d'une annonce sans détenir de compte, l'utilisateur se voyait communiquer en clair une référence confidentielle constituée de dix caractères alphanumériques dont les sept premiers étaient publics puisque correspondant aux caractères de la référence de l'annonce déposée sur le site. Cette référence confidentielle ne pouvait être modifiée par l'annonceur. Cette seule référence permettait à l'utilisateur d'accéder directement à l'annonce et à l'espace associé sur le site après l'avoir renseignée dans le champ correspondant. Par ailleurs, cette référence confidentielle qui s'apparente à un mot de passe était stockée en clair dans la base de données.

54. En défense, la société ne conteste pas en substance les manquements mais déclare avoir pris des actions correctives. Tout d'abord, elle annonce avoir adapté sa politique de mots de passe en exigeant des mots de passe d'une longueur de huit caractères composés d'au moins une majuscule, une minuscule, un chiffre et un caractère spécial. Elle rappelle que désormais les mots de passe sont hachés avec l'algorithme Bcrypt et que les mots de passe conservés en clair ont été supprimés. Ensuite, la société précise ne plus communiquer de références confidentielles aux utilisateurs exigeant la création d'un compte sur le site et avoir mis en place le blocage de l'espace propriétaire après dix tentatives de connexion infructueuses.

55. En premier lieu, la formation restreinte rappelle qu'il résulte des dispositions de l'article 32 du RGPD que le responsable de traitement est tenu de s'assurer que le traitement automatisé de données qu'il met en œuvre est suffisamment sécurisé. Le caractère suffisant des mesures de sécurité s'apprécie, d'une part, au regard des caractéristiques du traitement et des risques qu'il induit, d'autre part, en tenant compte de l'état de connaissances et du coût des mesures.

56. La formation restreinte considère tout d'abord que des règles de complexité des mots de passe trop permissives, qui autorisent l'utilisation de mots de passe insuffisamment robustes, peuvent conduire à des attaques par des tiers non autorisés, telles que des attaques par " force brute " ou " par dictionnaire ", qui consistent à tester successivement et de façon systématique de nombreux mots de passe et conduisent, ainsi, à une compromission des comptes associés et des données à caractère personnel qu'ils contiennent.

57. Elle relève, à cet égard, que la nécessité d'un mot de passe fort est recommandée tant par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) que par la Commission dans sa délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe, exigence confirmée dans sa délibération n° 2022-100 du 21 juillet 2022.

58. A titre d'illustration, la formation restreinte rappelle que la Commission considère dans sa délibération n° 2017-012 du 19 janvier 2017 – qui n'a certes pas un caractère impératif mais qui fournit un éclairage pertinent sur les mesures qu'il convient de prendre en matière de sécurité – que, pour assurer un niveau de sécurité et de confidentialité suffisant, dans l'hypothèse où l'authentification repose uniquement sur un identifiant et un mot de passe, ce dernier doit être composé d'au minimum douze caractères comprenant des majuscules, des minuscules, des chiffres et des caractères spéciaux.

59. À défaut, la Commission considère que permet également d'assurer un niveau de sécurité et de confidentialité suffisant une authentification reposant sur un mot de passe d'une longueur minimum de huit caractères, composé de trois catégories de caractères différentes mais accompagnée 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 (ex : " captcha ") et/ou le blocage du compte après plusieurs tentatives d'authentification infructueuses (au maximum dix).

60. La formation restreinte souligne qu'elle a adopté des sanctions pécuniaires où la caractérisation d'un manquement à l'article 32 du RGPD est le résultat de mesures insuffisantes pour garantir la sécurité des données traitées. Les délibérations n° SAN-2019-006 du 13 juin 2019, n° SAN-2019-007 du 18 juillet 2019 et n° SAN-2022-018 du 8 septembre 2022 visent notamment l'insuffisante robustesse des mots de passe.

61. La formation restreinte relève qu'en l'espèce, d'une part, les mots de passe des utilisateurs du site web www.pap.fr devaient être, à l'époque des contrôles, composé d'un caractère unique et dépourvus de mesure de sécurité complémentaire. Il ressort des observations de la société que les mots de passe exigés sont désormais d'une longueur de 8 caractères composés d'au moins une majuscule, une minuscule, un chiffre et un caractère spécial sans que soit prévue de restriction d'accès. D'autre part, les références confidentielles - assimilables à des mots de passe au sens de la définition de la délibération n° 2022-100 du 21 juillet 2022 selon laquelle le terme mot de passe désigne tout facteur de connaissance, à savoir tout ensemble d'informations révocable, connu uniquement de la personne concernée et permettant ou contribuant à l'authentification de celle-ci - étaient constituées de dix caractères alphanumériques dont les sept premiers étaient publics, en ce qu'ils correspondaient à la référence de l'annonce sur le site, avec seuls les trois derniers caractères privés. De plus, ces références étaient transmises en clair et ne pouvaient être modifiées par l'utilisateur de sorte qu'elles constituaient un moyen d'authentification pérenne.

62. La formation restreinte considère que de telles constructions ne permettent pas d'assurer la sécurité des données et d'empêcher que des tiers non autorisés y aient accès.

63. Concernant les mots de passe exigés au moment de la création d'un compte, elle rappelle, comme l'a souligné la rapporteure, que la société traitait au jour du contrôle sur place les données associées à près de cinq millions de comptes utilisateurs telles les nom, prénom, adresse électronique. Ainsi, ces mots de passe, associés à leurs identifiants, permettent d'accéder à toutes les données à caractère personnel contenues dans leurs comptes www.pap.fr. Ils n'étaient pas assez robustes, au regard des données personnelles en jeu et de l'état de l'art.

64. Concernant la référence confidentielle, la formation restreinte considère que l'usage de cette seule référence constituée de dix caractères alphanumériques ne remplissait pas le critère de complexité suffisant. En effet, il apparait qu'une première partie de cette référence, les sept premiers caractères alphanumériques correspondant à la référence de l'annonce, doit être assimilée un identifiant public. Quant à la seconde partie de la référence, composée des trois derniers caractères alphanumériques, qui s'apparente à un mot de passe ne remplit pas les critères de robustesse tels que décrits plus avant.

65. En outre, comme l'a souligné la rapporteure, cette référence confidentielle permet d'accéder aux données à caractère personnel présentes dans l'espace propriétaire associées à la personne ayant publié l'annonce, de les modifier et modifier également l'annonce. Au surplus, l'accès à cet espace permet d'accéder aux échanges intervenus entre le propriétaire et les personnes intéressées par l'annonce à l'occasion desquels de nombreuses informations personnelles peuvent être transmises (situations familiale, professionnelle, financière).

66. Aussi, une authentification reposant sur l'utilisation, d'une part, d'un mot de passe, par le passé court et dépourvu de mesure de sécurité complémentaire, actuellement toujours insuffisamment robuste en l'absence de mesure de sécurité complémentaire et, d'autre part, d'une référence confidentielle non modifiable, transmise en clair et sans complexité suffisante, peut conduire à des attaques par des tiers non autorisés et ainsi à une compromission des comptes utilisateurs et de " l'espace propriétaire " et des nombreuses données à caractère personnel qu'ils contiennent.

67. En conséquence, la formation restreinte considère que la politique des mots de passe et de la référence confidentielle déployée était et demeure insuffisamment robuste pour garantir la sécurité des données traitées, ce qui méconnaît l'article 32 du RGPD.

68. En deuxième lieu, la formation restreinte rappelle que la conservation des mots de passe de manière sécurisée constitue une précaution élémentaire en matière de protection des données à caractère personnel. Dès 2013, l'ANSSI alertait et rappelait les bonnes pratiques s'agissant de la conservation des mots de passe en indiquant qu'ils doivent " être stockés sous une forme transformée par une fonction cryptographique à sens unique (fonction de hachage) et lente à calculer telle que PBKDF2 " et que " la transformation des mots de passe doit faire intervenir un sel aléatoire pour empêcher une attaque par tables précalculées " (ANSSI, " Bulletin d'actualité CERTA-2013-ACT-046 ", 15 novembre 2013, https://www.cert.ssi.gouv.fr/actualite/CERTA-2013-ACT-046/).

69. De même, dans sa délibération n° 2017-012 du 19 janvier 2017, la CNIL indiquait déjà qu'elle " recommande [que le mot de passe] soit transformé au moyen d'une fonction cryptographique non réversible et sûre (c'est-à-dire utilisant un algorithme public réputé fort dont la mise en œuvre logicielle est exempte de vulnérabilité connue), intégrant l'utilisation d'un sel ou d'une clé ". En effet, les fonctions de hachage non robustes présentent des vulnérabilités connues qui ne permettent pas de garantir l'intégrité et la confidentialité des mots de passe en cas d'attaque par force brute après compromission des serveurs qui les hébergent.

70. En l'espèce, la formation restreinte relève que la conservation en clair, d'une part, des mots de passe d'utilisateurs, associés à leurs identifiants et à leur adresse électronique, et, d'autre part, des références confidentielles, associées à un espace personnel, ne permet pas de garantir leur sécurité. Cette modalité de conservation implique que toute personne ayant accès à la base de données des clients de la société – que ce soit un administrateur des systèmes d'information de la société ou un attaquant en cas de compromission – peut les consulter, les collecter, les modifier ou encore les vendre.

71. Dans ces conditions, la formation restreinte considère que les modalités de stockage des mots de passe et des références confidentielles ne permettaient pas, au jour des constats, de garantir la sécurité et la confidentialité des données à caractère personnel des détenteurs de comptes utilisateurs ce qui méconnaît l'article 32 du RGPD.

72. En conséquence, la formation restreinte considère que les faits précités, non contestés par la société, constituent des manquements aux obligations de l'article 32 du RGPD. Elle prend acte de ce que depuis les contrôles, la société a remédié partiellement aux manquements constatés en mettant en place une politique de mots de passe présentant un niveau de sécurité adéquat et en chiffrant l'ensemble des mots de passe.

2. Sur la conservation des données en base active

73. La rapporteure relève qu'à l'occasion des contrôles, la délégation a été informée que l'ensemble des données relatives aux clients inactifs était conservé durant dix ans et celles relatives aux comptes utilisateurs inactifs durant cinq ans en base active sans qu'intervienne d'archivage intermédiaire.

74. En défense, la société conteste l'existence du manquement. D'abord, elle fait valoir que cette conservation en base active des données des clients et utilisateurs devenus inactifs est justifiée par une finalité de lutte contre la fraude qui nécessite des contrôles quotidiens. Ensuite, elle précise que seules les personnes ayant un intérêt à traiter les données en raison de leurs fonctions peuvent accéder aux données à caractère personnel à savoir les conseillers du service client, les salariés des départements de l'informatique et les membres de la direction. A cet égard, elle ajoute que ces salariés sont soumis à une clause de confidentialité et à un engagement de confidentialité et que chacun d'eux dispose d'un mot de passe personnel.

75. La formation restreinte rappelle que pour assurer la sécurité des données, il est nécessaire qu'un tri soit effectué parmi ces données lorsqu'elles ne sont plus nécessaires à la finalité pour laquelle elles ont été collectées. Ainsi, elles doivent être supprimées ou faire l'objet d'un archivage intermédiaire consistant notamment en une séparation physique ou logique.

76. Dans le présent cas, la formation restreinte relève qu'il ressort des explications fournies par la société que si la finalité de lutte contre la fraude peut justifier une conservation des données, les modalités de conservation des données en base active telles que définies par la société ne permettent pas d'assurer la sécurité des données. D'une part, la formation restreinte relève le nombre important de catégories de salariés ayant accès à la base de données dans la mesure où aussi bien les conseillers du service client, les salariés des départements de l'informatique que les membres de la direction sont habilités à accéder à la base de données. D'autre part, elle constate l'absence de tri opéré entre les données conservées alors qu'il apparaît que la conservation des données telles que celles de l'annonce et de l'adresse de facturation n'est pas nécessaire à l'objectif poursuivi de lutte contre la fraude. La société a en effet confirmé lors de la séance que la donnée utilisée afin d'identifier des fraudeurs était l'adresse électronique.

77. En conséquence, la formation restreinte considère que le manquement est constitué.

F. Sur le manquement à l'obligation d'information et au droit d'opposition à la prospection commerciale par courrier électronique pour produits ou services analogues

78. L'article L. 34-5 du code des postes et des communications électroniques (CPCE) prévoit que " Est interdite la prospection directe au moyen de système automatisé de communications électroniques […], d'un télécopieur ou de courriers électroniques utilisant les coordonnées d'une personne physique […] qui n'a pas exprimé préalablement son consentement à recevoir des prospections directes par ce moyen.

Constitue une prospection directe l'envoi de tout message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services. Pour l'application du présent article, les appels et messages ayant pour objet d'inciter l'utilisateur ou l'abonné à appeler un numéro surtaxé ou à envoyer un message textuel surtaxé relèvent également de la 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 ".

79. Ces dispositions transposent en droit français les règles régissant l'utilisation de systèmes automatisés d'appel et de communication sans intervention humaine (automates d'appel), de télécopieurs ou de systèmes d'envoi de courrier électronique à des fins de prospection directe fixées par 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 (dite directive " ePrivacy "), telle que modifiée par la directive 2009/136/CE du 25 novembre 2009.

80. La rapporteure relève que lorsqu'un utilisateur souscrit à une alerte concernant un bien immobilier, celui-ci est susceptible de recevoir des courriels pour des biens ou services analogues par la société, sans en avoir été ni informé ni avoir eu la possibilité de s'y opposer, lors de la création de l'alerte.

81. En défense, la société conteste le manquement en affirmant que les courriers électroniques litigieux ne constituent pas de la prospection commerciale puisqu'ils ne visent pas à promouvoir des biens ou services. En outre, elle fait valoir le faible volume de ce type de messages et précise que les utilisateurs ont la possibilité de se désinscrire via un lien de désinscription présent dans chaque nouvelle communication.

82. La formation restreinte rappelle qu'au sens de l'article L.34-5 du CPCE, d'une part, la prospection commerciale directe se définit comme " tout message visant la promotion directe ou indirecte de biens, services ou de l'image d'une personne vendant des biens ou fournissant des services ". D'autre part, les produits et services analogues, proposés à l'occasion d'une vente ou d'une prestation de services, doivent s'entendre comme promouvant des biens ou services d'une même personne physique ou morale sans nécessité que la promotion conduise à une transaction financière avec la personne.

83. La formation restreinte considère que les courriels adressés par la société aux utilisateurs tels que ceux contenant des informations concernant une annonce ou des sondages anonymes sur des actualités immobilières découlent directement de la souscription à l'alerte relative à un bien immobilier et ne visent pas à promouvoir d'autres biens ou services proposés par la société. Aussi, ces courriels ne constituent pas de la prospection commerciale au sens de l'article L.34-5 du CPCE.

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

III. Sur les mesures correctrices et leur publicité

85. 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 : […] 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. "

86. L'article 83 du RGPD prévoit que " Chaque autorité de contrôle veille à ce que les amendes administratives imposées […] soient, dans chaque cas, effectives, proportionnées et dissuasives ", avant de préciser les éléments 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.

A. Sur le prononcé d'une amende administrative et son montant

1. Sur le prononcé d'une amende administrative

87. En défense, la société considère que l'amende administrative proposée est disproportionnée par rapport aux manquement allégués et à sa conduite puisqu'elle a mis en œuvre plusieurs mesures correctives avant la fin de l'instruction, en particulier, la modification de sa politique de confidentialité afin de délivrer les informations requises, le recours à des sous-traitants encadré par un acte juridique contenant l'ensemble des mentions prévues, la mise en place d'une politique et de stockage de mot de passe présentant un niveau de sécurité adéquat. En outre, elle souligne avoir pleinement coopéré avec les services de la CNIL. Elle ajoute qu'elle n'a tiré aucun avantage financier des manquements reprochés. Elle fait valoir que son chiffre d'affaires stagne et que le secteur immobilier, particulièrement concurrentiel, est en crise. Enfin, elle considère que l'amende de 250 000 euros proposée par la rapporteure équivaut à […] % de son chiffre d'affaires de 2023 et est, par conséquent, excessive.

88. 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, la portée ou la finalité du traitement concerné, le nombre de personnes affectées, les mesures prises par le responsable du traitement pour atténuer le dommage subi par les personnes concernées, le fait que la violation a été commise par négligence, le degré de coopération avec l'autorité de contrôle et, dans certains cas, le niveau de dommage subi par les personnes.

89. La formation restreinte relève d'abord que les manquements reprochés à la société portent atteinte à des principes fondamentaux prévus par le RGPD et concernent de nombreuses personnes.

90. S'agissant du manquement au principe de limitation de la durée de conservation des données à caractère personnel, la société a fait preuve de négligence, d'une part, en ne définissant pas de façon adéquate une durée de conservation relative aux données des clients ayant conclu un contrat inférieur à 120 euros et, d'autre part, en n'appliquant pas la durée de conservation qu'elle avait définie pour les données relatives aux utilisateurs au jour des contrôles. La formation restreinte relève que ce manquement concerne un nombre important de personnes, la société dénombrant 2 394 538 utilisateurs dont la dernière connexion à leur compte remontait entre cinq et dix ans à la date des contrôles.

91. S'agissant du manquement à l'obligation d'information des personnes concernées et à la transparence, la formation restreinte relève que la société a manqué à l'exigence de fourniture d'une information complète et transparente aux personnes concernées, qui constitue un préalable indispensable à tout traitement de données à caractère personnel.

92. S'agissant du manquement à l'obligation d'encadrer par un acte juridique formalisé les traitements effectués pour le compte du responsable de traitement, la formation restreinte relève que la société a manqué de rigueur en ne veillant pas à souscrire à un document contractuel contenant les mentions requises à l'article 28 du RGPD, privant ainsi les personnes concernées de bénéficier d'une pleine protection de leurs données à caractère personnel.

93. S'agissant du manquement à l'obligation d'assurer la sécurité des données à caractère personnel, la formation restreinte souligne le nombre de manquements constatés aux obligations élémentaires de sécurité, à savoir, le recours à un mot de passe et à une référence confidentielle insuffisamment robustes pour des comptes clients ou utilisateurs, la transmission en clair de la référence confidentielle, le stockage en clair des mots de passe et références confidentielles ainsi que la conservation des données en base active. La formation restreinte estime que l'accumulation de ces défauts de sécurité ne permettait pas aux personnes de bénéficier de l'entière protection prévue par le RGPD quant à l'usage de leurs données.

94. Enfin, tout en tenant compte de ce que la société a mis en place des mesures à la suite de la notification du rapport de sanction, la formation restreinte relève que ces actions n'exonèrent pas la société de sa responsabilité pour les manquements constitués pour le passé.

95. En conséquence, la formation restreinte considère qu'il y a lieu de prononcer une amende administrative pour les manquements aux articles 5-1-e), 13, 28 et 32 du RGPD.

2. Sur le montant de l'amende administrative

96. La formation restreinte relève d'abord que les manquements aux articles 5-1-e) et 13 du RGPD constituent des manquements à des principes clés du RGPD susceptibles de faire l'objet, en vertu de l'article 83 du RGPD, d'une amende administrative pouvant s'élever jusqu'à 20 000 000 euros ou jusqu'à 4 % du chiffre d'affaires annuel, le montant le plus élevé étant retenu.

97. La formation restreinte relève que la société a réalisé, en 2022, un chiffre d'affaires d'environ […] d'euros pour un résultat net de […].

98. Dès lors, au regard de la responsabilité de la société, de ses capacités financières et des critères pertinents de l'article 83 du Règlement, la formation restreinte estime qu'une amende administrative d'un montant total de cent mille (100 000) euros pour les manquements aux articles 5-1-e), 13, 28 et 32 du RGPD apparait justifiée.

B. Sur la publicité

99. La formation restreinte considère que la publicité de la présente décision se justifie au regard de la gravité des manquements en cause et du nombre de personnes concernées. Elle considère également que la publicité de la sanction permettra notamment d'informer l'ensemble des personnes concernées par les manquements.

100. Enfin, la mesure est proportionnée dès lors que la décision n'identifiera plus nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

PAR CES MOTIFS

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

• prononcer à l'encontre de la société DE PARTICULIER A PARTICULIER – EDITIONS NERESSIS une amende administrative d'un montant de cent mille (100 000) euros pour manquements aux articles 5-1-e), 13, 28 et 32 du règlement (UE) n° 2016/679 du 27 avril 2016 relatif à la protection des données ;

• 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

Cette décision est susceptible de faire l'objet d'un recours devant le Conseil d'État dans un délai de deux mois à compter de sa notification.