Délibération SAN-2023-006 du 11 mai 2023

Commission Nationale de l'Informatique et des Libertés Etat juridique : En vigueur

Date de publication sur Légifrance : Mercredi 17 mai 2023

Délibération de la formation restreinte no SAN-2023-006 du 11 mai 2023 concernant la société DOCTISSIMO

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de Monsieur Philippe-Pierre CABOURDIN, vice-président, Madame Christine MAUGÜÉ, Madame Anne DEBET, Monsieur Alain DRU 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 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 saisine no 20010597 ;

Vu la décision n° 2020-123C du 14 août 2020 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 accessibles à partir du nom de domaine " doctissimo.fr ", et tout traitement lié ;

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 29 novembre 2021 ;

Vu le rapport de Madame Valérie PEUGEOT, commissaire rapporteure, notifié à la société DOCTISSIMO le 19 juillet 2022 ;

Vu les observations écrites versées par la société DOCTISSIMO le 5 octobre 2022 ;

Vu la réponse de la rapporteure à ces observations, notifiée le 21 novembre 2022 au conseil de la société ;

Vu les observations écrites versées par la société DOCTISSIMO le 5 janvier 2023 ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 9 février 2023 :

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

En qualité de représentants de la société DOCTISSIMO :

[...]

La société DOCTISSIMO ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. La société DOCTISSIMO (ci-après " la société "), dont le siège social est situé 1 Quai du Point du Jour à BOULOGNE-BILLANCOURT (92100), est une filiale détenue à 100% par la société UNIFY. Elle a été immatriculée au registre du commerce et des sociétés le 17 novembre 1994 et la délégation a été informée qu'elle a été créée en mai 2000. Elle employait, en 2020,

une trentaine de salariés. Elle a réalisé, en 2020, un chiffre d'affaires d'environ [...], pour un résultat net d'environ [...] puis en 2021, un chiffre d'affaires d'environ [...], pour un résultat net négatif de [...].

2. La société UNIFY était détenue directement par le groupe de médias français TF1 jusqu'au 28 juin 2022, date à laquelle le groupe TF1 a cédé au groupe REWORLD MEDIA " les actifs média et des activités digitales du pôle Publishers de [la société] UNIFY ", dont fait partie la société DOCTISSIMO.

3. La société DOCTISSIMO édite le site web francophone www.doctissimo.fr (ci-après " le site web "), qui propose principalement des articles, tests, quiz et forums de discussion en lien avec la santé et le bien-être. Le site web de la société est disponible uniquement en langue française mais est accessible à partir de l'ensemble des pays de l'Union européenne et également hors de l'Europe. La société DOCTISSIMO revendiquait environ […] de visiteurs uniques du site web entre les mois de mai 2021 et avril 2022 et environ […] utilisateurs inscrits, disposant d'un compte utilisateur créé à partir du site web doctissimo.fr, à la date du 8 avril 2022. Les utilisateurs, inscrits ou visiteurs, sont situés majoritairement en France et en Belgique. Enfin, la société comptabilise environ […] utilisateurs ayant répondu à au moins une question d'un questionnaire ayant pour thème la santé entre les mois de février 2020 et janvier 2021. La délégation a été informée que parmi ces utilisateurs, […] sont situés en France et […] sont situés en Belgique.

4. Le 26 juin 2020, la Commission nationale de l'informatique et des libertés (ci-après " la CNIL " ou " la Commission ") a été saisie d'une plainte n° […] par l'association PRIVACY INTERNATIONAL concernant l'ensemble des traitements de données à caractère personnel des utilisateurs mis en œuvre par la société DOCTISSIMO sur son site web et, en particulier, les modalités de dépôt des cookies sur le terminal des utilisateurs lorsqu'ils se rendent sur le site web ; la base légale du traitement des données à caractère personnel des utilisateurs susceptibles d'être collectées sur le site web quand un utilisateur effectue des tests ayant pour thème la santé ; l'obligation de transparence et de fourniture d'informations aux utilisateurs du site web ainsi que la sécurité des données des utilisateurs.

5. L'association PRIVACY INTERNATIONAL ayant publiquement communiqué sur sa plainte, la société DOCTISSIMO a apporté des précisions à la connaissance de la CNIL par courrier du 7 juillet 2020 en indiquant notamment, ne procéder à aucun dépôt de cookies et autres traceurs avant le consentement de l'utilisateur et travailler à la mise en place d'un consentement pour l'accès aux tests susceptibles de révéler les catégories particulières de données.

6. Quatre missions de contrôle ont eu lieu en application de la décision n° 2020-123C du 14 août 2020 de la Présidente de la CNIL. Le 9 septembre 2020, les services de la CNIL ont d'abord effectué un contrôle en ligne à partir du domaine www.doctissimo.fr. Le 1er octobre 2020, les services de la CNIL ont ensuite procédé à un contrôle sur place de la société DOCTISSIMO, dans ses locaux située 8 rue Saint-Fiacre à Paris (75002), avant d'effectuer, le 1er décembre 2020, un nouveau contrôle en ligne à partir du domaine " doctissimo.fr ". Enfin, le 8 février 2021, un contrôle sur pièces a été effectué par l'envoi d'un questionnaire adressé à la société.

7. Ces missions ont donné lieu à l'établissement des procès-verbaux n° 2020-123/1, 2020-123/2 et 123/3 et à des courriers et informations communiquées par la société les 13 et 21 octobre 2020, 19 novembre 2020, 8 décembre 2020, 18 janvier 2021 et 24 février 2021.

8. Ces missions ont eu pour principal objet d'instruire la plainte dont la CNIL était saisie et de procéder à la vérification de la conformité des traitements de données à caractère personnel accessibles à partir du nom de domaine " doctissimo.fr ", ainsi que de tout traitement lié, aux dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après " le RGPD ") 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 ").

9. Conformément à l'article 56 du RGPD, le 3 décembre 2020, la CNIL a informé 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 principal de la société se trouve en France. Après échange entre la CNIL et les autorités de protection des données européennes dans le cadre du mécanisme de guichet unique, celles-ci sont toutes concernées par le traitement puisque le site web comporte des visiteurs de tous les États membres de l'Union européenne.

10. Le 8 avril 2021, la société DOCTISSIMO a formulé auprès de la CNIL une demande de conseil et d'accompagnement. Il lui a été répondu le 30 avril 2021, que la charte d'accompagnement des professionnels prévoit une impossibilité d'accompagner les organismes dans leur mise en conformité lorsqu'une procédure de contrôle est en cours.

11. Le 27 octobre 2021, la société DOCTISSIMO a fait parvenir à la CNIL un courrier reprenant les actions en lien avec les traitements de données à caractère personnel accessibles depuis le domaine " doctissimo.fr " et tout traitement lié, réalisées par la société DOCTISSIMO depuis le mois de juillet 2020.

12. Aux fins d'instruction de ces éléments, la présidente de la Commission a, le 29 novembre 2021, désigné Madame Valérie PEUGEOT en qualité de rapporteure sur le fondement de l'article 22 de la loi du 6 janvier 1978 modifiée.

13. À l'issue de son instruction, la rapporteure a, le 19 juillet 2022, fait notifier à la société un rapport détaillant les manquements aux articles 5-1-e), 9, 13, 26 et 32 du RGPD et à l'article 82 de la loi Informatique et Libertés qu'elle estimait constitués en l'espèce. Ce rapport proposait à la formation restreinte de prononcer une amende administrative à l'encontre de la société, ainsi qu'une injonction, assortie d'une astreinte de mettre en conformité le traitement avec les dispositions des articles 5-1-e) et 32 du RGPD et de l'article 82 de la loi. Ce rapport proposait également que cette décision soit rendue publique mais ne permette plus d'identifier nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

14. Le 5 octobre 2022, la société a produit ses observations en réponse au rapport de sanction.

15. La rapporteure a répondu aux observations de la société le 21 novembre 2022.

16. Le 5 janvier 2023, la société a produit de nouvelles observations en réponse à celles de la rapporteure.

17. Par courrier du 19 janvier 2023, la rapporteure a informé le conseil de la société que l'instruction était close, en application de l'article 40, III, du décret modifié n°2019-536 du 29 mai 2019.

18. Par courrier du 19 janvier 2023, la société a été informée que le dossier était inscrit à l'ordre du jour de la formation restreinte du 9 février 2023.

19. 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

20. En application de l'article 60 paragraphe 3 du RGPD, le projet de décision adopté par la formation restreinte a été transmis le 30 mars 2023 aux autorités de contrôle européennes concernées.

21. Au 27 avril 2023, 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 conserver les données à caractère personnel pour une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées en application de l'article 5, paragraphe 1, e) du RGPD

22. 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 ; 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) ".

a. Sur les durées de conservation des données relatives aux tests et aux " quizz " réalisés par les utilisateurs du site web doctissimo.fr

23. La rapporteure a relevé que la délégation a constaté lors des contrôles des 9 septembre, 1er octobre et 1er décembre 2020 que des tests et des " quizz " (ci-après " des questionnaires " ou " des tests ") étaient disponibles sur le site web de la société. Lors du contrôle du 1er octobre 2020, la délégation a été informée que ces questionnaires étaient rédigés par la société mais que leur mise en œuvre et leur hébergement étaient réalisés par un sous-traitant, la société [...].

24. En premier lieu, la rapporteure relève que jusqu'au 11 octobre 2020, la société [...] conservait les réponses issues des tests effectués par l'ensemble des utilisateurs loggés et non loggés ainsi que l'adresse IP de ces derniers pendant une durée de 24 mois à compter de leur réalisation. La rapporteure a ainsi relevé qu'un fichier contenait les réponses issues des tests effectués par les utilisateurs au sujet du cancer du côlon, associées à leur adresse IP.

25. La rapporteure relève ensuite qu'une mention située en-dessous des questionnaires portant sur des sujets de santé indique que la réalisation d'un test permet à l'utilisateur d'en connaitre le résultat et, le cas échéant, de le partager avec ses amis. Cela permet également à la société DOCTISSIMO de réaliser des statistiques agrégées sur l'utilisation des tests.

26. S'agissant des deux premières finalités, la rapporteure observe qu'il ressort des constats effectués que le résultat du test s'affiche immédiatement à la fin du déroulement des questions posées. Elle considère, dès lors, que la conservation des réponses de l'utilisateur au questionnaire ainsi que de son adresse IP n'apparait pas nécessaire après la communication du résultat à l'utilisateur et son éventuel partage par ce dernier avec ses amis. Ces finalités ne sauraient en tous cas justifier une conservation d'une durée de 24 mois des données à caractère personnel concernées.

27. S'agissant de la troisième finalité, la rapporteure observe qu'en l'espèce les statistiques agrégées sont réalisées indépendamment des réponses aux questionnaires, aux moyens d'outils de mesure d'audience, qui impliquent notamment le dépôt et / ou la lecture de cookies ou autres traceurs sur le terminal de l'utilisateur ayant pour finalité la mesure d'audience et l'utilisation de l'adresse IP de l'utilisateur. Elle considère, dès lors, que la conservation des réponses aux questionnaires après la fin du test n'est pas nécessaire à la réalisation des statistiques agrégées sur l'utilisation des tests, qui s'effectue au fil de l'eau par d'autres moyens.

28. En second lieu, la rapporteure relève que depuis le 11 octobre 2020, la société DOCTISSIMO a demandé à la société [...], d'anonymiser les données relatives aux tests et " quizz " dès leur collecte. La société DOCTISSIMO indique que depuis cette date, son sous-traitant procède à un hachage des adresses IP - pour lesquelles la société indique qu'il s'agit des " seules données identifiantes auxquelles sont rattachées les informations relatives aux participations " - avec l'algorithme HMAC-SHA256 et que l'ensemble des données relatives à des participations aux tests datant de plus de trois mois à compter de leur réalisation a fait l'objet d'une suppression afin de répondre aux trois finalités susmentionnées. Au regard des éléments communiqués par la société, la rapporteure a relevé que, l'algorithme de hachage utilisé par la société [...] correspond en réalité seulement à une fonction SHA256, sans clé de hachage. La rapporteure relève que l'usage seul de la fonction SHA256, s'il permet d'assurer l'intégrité des données à caractère personnel, ne permet pas d'assurer leur anonymisation.

29. En défense, la société soutient que le manquement reproché est involontaire puisqu'il résulte de la mauvaise exécution du contrat conclu avec son sous-traitant qui n'a pas respecté ses obligations contractuelles relatives à la suppression des données provenant des tests à l'issue de leur affichage d'une part, et celles prévoyant le recours à une variable aléatoire dans la fonction d'anonymisation des adresses IP d'autre part. La société DOCTISSIMO précise avoir mis fin au contrat qui

la liait avec [...] dès le 16 mars 2021. Ensuite, la société soutient que la rapporteure invoque une possession hypothétique des informations permettant la réidentification et que le risque d'attaque en termes de probabilité et de gravité n'est pas qualifié. Elle considère que la vraisemblance du risque d'attaque de ses propres systèmes par [...] est négligeable et que sa gravité serait très limitée en l'absence de données sensibles. Enfin, la société DOCTISSIMO conclut qu'à compter du 11 octobre 2020, les données des tests ne contenaient que des données non identifiantes et que ces dernières pouvaient être conservées sans limitation de durée.

30. En premier lieu, la formation restreinte rappelle que la durée de conservation des données à caractère personnel doit être déterminée en fonction de la finalité poursuivie par le traitement et que lorsque cette finalité est atteinte, les données doivent par principe être supprimées ou anonymisées.

31. En l'espèce, la formation restreinte relève qu'il n'est pas contesté par la société qu'avant le 11 octobre 2020, le sous-traitant de la société DOCTISSIMO conservait les réponses issues des tests réalisés par les utilisateurs ainsi que leur adresse IP, pendant 24 mois à compter de leur réalisation. La formation restreinte considère que la conservation des réponses de l'utilisateur au questionnaire ainsi que de son adresse IP n'apparait pas nécessaire après la communication du résultat à l'utilisateur et son éventuel partage par ce dernier avec ses amis. De même, la conservation des réponses aux questionnaires après la fin du test ainsi que de son adresse IP n'est pas nécessaire à la réalisation des statistiques agrégées sur l'utilisation des tests dès lors qu'elles peuvent, et sont en l'espèce, effectuées au fil de l'eau aux moyens d'outils de mesure d'audience. À cet égard, la formation restreinte note que la société ne justifie pas d'une nécessité de conservation de ces données.

32. La formation restreinte note que le contrat de sous-traitance prévoyait que les adresses IP des participants ne devaient pas être collectées par [...] concernant les " quiz anonymes dits " sensibles " ". Néanmoins, la formation restreinte relève que la société DOCTISSIMO avait accès à des tableaux de bord, établis par son sous-traitant, comprenant les réponses des participants aux tests et aux " quizz " ainsi que leurs adresses IP sous forme pseudonymisée. La formation restreinte relève que ce n'est qu'à la suite de la plainte de l'association PRIVACY INTERNATIONAL que la société DOCTISSIMO a interrogé son sous-traitant afin de connaître les mesures qu'il mettait en œuvre, alors qu'elle avait connaissance de la collecte des adresses IP par ce dernier, via lesdits tableaux de bord. Ensuite, la formation restreinte relève que, si la société DOCTISSIMO a sollicité de son sous-traitant qu'il procède à la suppression des résultats des tests dès l'affichage, elle ne s'est pas opposée à la solution alternative proposée par la société [...], consistant à procéder à compter du 11 octobre 2020, à la seule anonymisation des adresses IP.

33. Si le responsable de traitement peut décider de recourir à un prestataire spécialisé, en particulier en lui confiant une mission de sous-traitance des données à caractère personnel, au sens du RGPD, il reste tenu de veiller, par des diligences raisonnables, à ce que le respect de la protection des données à caractère personnel soit effectivement assuré. Le caractère suffisant de ces diligences dépend notamment des compétences et des moyens du responsable de traitement. La formation restreinte rappelle que la responsabilité du responsable de traitement peut être retenue du fait de l'absence de mise en œuvre par celui-ci d'un contrôle régulier sur les mesures techniques et organisationnelles prises par son sous-traitant (CE, 10ème chambre, 26 avril 2022, Société Optical Center, n° 449284). La formation restreinte a notamment retenu la responsabilité d'un responsable de traitement pour ne pas avoir exercé un contrôle suffisant sur la prestation réalisée en considérant qu'un simple engagement contractuel de son courtier visant à " respecter le RGPD et les règles applicables en matière de prospection commerciale " n'est pas une mesure suffisante, dans sa délibération SAN-2022-021 du 24 novembre 2022 à l'encontre de la société […].

34. Il résulte de ce qui précède que la formation restreinte considère que la société DOCTISSIMO, qui constitue une société qui dispose de compétences dans le domaine du numérique, n'a pas suffisamment suivi l'exécution de ses instructions contractuelles par son sous-traitant et n'a pas exercé un contrôle satisfaisant sur les mesures techniques et organisationnelles qu'il mettait en œuvre pour assurer la conformité au RGPD et, notamment pour assurer l'absence de collecte de données à caractère personnel ou encore l'anonymisation de celles-ci. Par ailleurs, la formation restreinte relève que les données en question et les adresses IP des utilisateurs étaient accessibles à la société DOCTISSIMO.

35. En conséquence, la formation restreinte considère que les faits précités constituent un manquement à l'article 5-1-e) du RGPD dès lors que, jusqu'au 11 octobre 2020, les réponses aux tests et " quizz " ainsi que les adresses IP, pouvant être associées aux informations des comptes utilisateurs étaient conservées pendant une durée de vingt-quatre mois à compter de leur réalisation, ce qui excédait les finalités pour lesquelles les données étaient traitées.

36. En second lieu, la formation restreinte relève que depuis le 11 octobre 2020, la société [...] procède à un hachage des adresses IP avec la fonction SHA256 sans clé de hachage, et que l'ensemble des données relatives à des participations aux tests datant de plus de trois mois à compter de leur réalisation a fait l'objet d'une suppression.

37. La formation restreinte relève que la Commission a communiqué publiquement sur son site internet sur l'usage de la fonction SHA256. La Commission a ainsi considéré que, s'il permet d'assurer l'intégrité des données à caractère personnel, l'usage de la fonction SHA256 sans clé de hachage associée, ne permet pas d'assurer leur anonymisation. La formation restreinte considère donc que la fonction de hachage utilisée par le sous-traitant de la société DOCTISSIMO ne saurait constituer une solution d'anonymisation mais seulement de pseudonymisation des données à caractère personnel des utilisateurs, en ce que la société [...] qui connaissait les paramètres du hachage, et compte tenu du fait que le nombre d'adresses IP est connu et limité, pouvait retrouver par force brute et dans un délai raisonnable, l'adresse IP des personnes ayant répondu aux tests.

38. Dès lors que les données relatives à la participation d'utilisateurs aux tests et " quizz " ne sont pas anonymisées, la formation restreinte considère, comme elle l'a précédemment développé, que leur conservation n'apparait pas nécessaire après la communication du résultat à l'utilisateur et son éventuel partage puisque le résultat du test s'affiche immédiatement à la fin du déroulement des questions posées. De même, la formation restreinte considère que leur conservation n'est pas nécessaire à la réalisation des statistiques agrégées sur l'utilisation des tests. La formation restreinte considère donc que la société ne justifie d'aucune nécessité de conservation de ces données pendant une durée de trois mois.

39. En conséquence, la formation restreinte considère que les faits précités constituent un manquement à l'article 5-1-e) du RGPD pour les faits relevés à compter du 11 octobre 2020 dès lors que les réponses aux tests et " quizz " sont conservées pendant une durée de trois mois à compter de leur réalisation du fait d'une procédure d'anonymisation ineffective des adresses IP, ce qui excède la durée nécessaire aux finalités pour lesquelles elles sont traitées.

40. La formation restreinte relève qu'au cours de la procédure, la société DOCTISSIMO a indiqué s'être mise en conformité avec les exigences de l'article 5-1-e) puisque depuis le 16 mars 2021, son sous-traitant ne collecte plus les adresses IP des utilisateurs, de sorte qu'il n'y a pas lieu à adresser d'injonction à la société sur ce point. La formation restreinte considère néanmoins le manquement constitué pour les faits passés.

b. Sur les durées de conservation des comptes créés par les utilisateurs du site doctissimo.fr

41. La rapporteure relève qu'il ressort du référentiel relatif aux durées de conservation de la société qu'elle anonymise " les données relatives au compte membre après 3 ans d'inactivité ". La rapporteure relève également que lors du contrôle sur place du 1er octobre 2020, la délégation a été informée qu'après trois ans d'inactivité, les " informations directement identifiantes des comptes sont supprimées ou remplacées par des données aléatoires aux fins d'anonymisation ". Or, la rapporteure relève que la procédure d'anonymisation mise en place par la société ne satisfait pas au critère d'impossibilité d'individualisation du fait de la conservation de l'identifiant unique de l'utilisateur, " id_user ", et de son nom d'utilisateur pseudonymisé qui permet une ré-identification indirecte de ce dernier.

42. La rapporteure considère que la procédure mise en place par la société ne constitue pas une solution d'anonymisation, mais une simple pseudonymisation des données de l'utilisateur.

43. En défense, la société ne conteste pas que l'identifiant unique de l'utilisateur, " id_user ", est conservé. Néanmoins, la société considère qu'il ne permet pas de réidentifier les titulaires du compte puisqu'il n'est lié à aucune autre donnée et que le pseudonyme des utilisateurs est anonymisé après 3 ans d'inactivité en étant remplacé par une suite de chiffres et de lettres aléatoires. La société DOCTISSIMO soutient donc que la possibilité et le risque de la réidentification des personnes n'est pas démontrée. Enfin, la société a indiqué mettre en place une nouvelle procédure d'anonymisation de tous les comptes des utilisateurs inactifs depuis plus de 3 ans à compter de la fin du mois d'octobre 2022. Elle précise à cet égard que les identifiants uniques des utilisateurs inactifs depuis plus de 3 ans et les pseudonymes seront supprimés, y compris ceux présents sur les forums et ceux figurant dans les publications d'autres membres du forum.

44. La formation restreinte rappelle que la pseudonymisation de données à caractère personnel est une opération réversible et qu'il est possible de retrouver l'identité d'une personne en disposant d'informations supplémentaires.

45. La formation restreinte relève en l'espèce que la société ne conteste pas que sa politique d'anonymisation des données prévoyait, concernant les comptes inactifs depuis plus de 3 ans, la conservation de l'identifiant unique des utilisateurs, " id_user ", ainsi que de leur nom d'utilisateur pseudonymisé. Or, la formation restreinte considère que la conservation de l'identifiant unique, " id_user " de l'utilisateur, associée à son nom d'utilisateur pseudonymisé n'empêchait pas de relier les données associées aux comptes. La formation restreinte relève ainsi que la procédure mise en place par la société permettait la conservation des données non identifiantes associées aux comptes, telles que les publications sur les forums ; or, la formation restreinte estime qu'il est courant que les utilisateurs communiquent entre eux en utilisant leurs noms d'utilisateurs. La formation restreinte considère qu'il était donc possible en l'espèce, de retrouver l'identité d'une personne en disposant d'informations supplémentaires.

46. En conséquence, la formation restreinte considère que les faits précités constituent un manquement à l'article 5-1-e) du RGPD dès lors que les mesures prises par la société pour anonymiser correctement les données à caractère personnel de l'utilisateur à l'issue d'un délai de trois ans ne correspondaient pas à une anonymisation mais à une simple pseudonymisation des données. La formation restreinte relève que la société s'est mise en conformité au cours de la procédure avec la mise en place d'une nouvelle procédure d'anonymisation, de sorte qu'il n'y a pas lieu à adresser d'injonction à la société sur ce point, mais elle rappelle néanmoins que cela ne saurait exonérer la société de sa responsabilité pour le passé.

C. Sur le manquement à l'obligation de recueillir le consentement des personnes concernées au traitement de catégories particulières de données à caractère personnel en application de l'article 9 du RGPD

47. Aux termes de l'article 9 du RGPD, le traitement des données à caractère personnel qui révèle des données concernant la santé d'une personne physique est interdit sauf s'il relève d'une des conditions prévues à l'article 9-2-a) à j) du RGPD.

48. Aux termes de l'article 4-15 du RGPD, les " données concernant la santé " sont " les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique […] ".

49. La rapporteure relève qu'il ressort des constatations effectuées à l'occasion des contrôles des 9 septembre, 1er octobre et 1er décembre 2020 que la société traite des données de santé lorsque les personnes répondent aux différents questionnaires ayant pour thème la santé qui leur sont proposés sur le site doctissimo.fr.

50. La rapporteure relève ensuite que la délégation a constaté lors de son contrôle en ligne du 9 septembre 2020 que la société ne recueillait pas l'accord de l'internaute sur l'utilisation de ses données " sensibles " afin de procéder au traitement de ses données relatives à sa santé puisque seul un texte comprenant un lien vers la politique de protection des données personnelles figurait en dessous du test.

51. La rapporteure relève néanmoins que la délégation a été informée, par courrier du 19 novembre 2020, que les tests susceptibles d'engendrer la collecte de données de santé ont été retirés du site le 12 septembre 2020. Ces tests sont de nouveau accessibles depuis le 15 octobre 2020 et leur participation est conditionnée au fait que les internautes consentent, au moyen d'une case à cocher, au traitement de leurs informations. La rapporteure relève qu'il ressort des constatations du 1er décembre 2020 que la case à cocher est accompagnée de la mention suivante " J'accepte que les

éventuelles données sensibles que je renseigne au travers de mes réponses au test soient utilisées tel que décrit ci-dessous et détaillé dans la Politique de protection des données personnel ".

52. En défense la société soutient tout d'abord que le champ matériel de la notion de données de santé n'est pas défini par le RGPD et que son imprécision a conduit la société à solliciter, en vain, le conseil de la CNIL plus de 6 mois avant la désignation de la rapporteure, le 8 avril 2021. Ensuite, la société soutient que la rapporteure n'a pas apporté la preuve du traitement systématique de données de santé par DOCTISSIMO en violation de l'article 6 de la CEDH. La société soutient que, n'ayant accès qu'aux adresses IP hachées des utilisateurs, elle ne peut pas identifier les personnes concernées. Enfin, seule une part très minoritaire des tests proposés sur le site internet de DOCTISSIMO, de l'ordre de 5%, serait susceptible de permettre la collecte des données de santé, à supposer que cette qualification juridique soit effectivement applicable.

53. En premier lieu, la formation restreinte considère que le fichier démontrant la collecte des réponses des utilisateurs à un test intitulé " Cancer du côlon : quels sont vos risques " associées à leurs adresses IP permet de constater la collecte d'informations concernant les antécédents médicaux (cancer du sein ou de l'endomètre) ou l'état physiologique des personnes concernées (indice de masse corporelle). La formation restreinte relève que la société proposait d'autres tests accessibles sur son site web et portant sur le thème de la santé, tels que notamment, les tests intitulés " où en êtes-vous avec l'alcool ? ", " manquez-vous de fer ? ", " mangez-vous trop de sucre ? ", " Et si c'était de l'asthme ? ", " Varices : êtes-vous à risque ? ", " Et si c'était la maladie d'Alzheimer ? ", " Accident vasculaire cérébral : quels sont vos risques ? ", " Patients hypertendus : faites-vous assez de sport ? " ou encore " Avez-vous une bonne audition ?.

54. La formation restreinte relève qu'il a été démontré que le système de hachage des adresses IP mis en place ne permettait pas d'empêcher la réidentification des utilisateurs du site web et que la société DOCTISSIMO était en mesure d'associer les réponses issues des tests effectués à l'adresse IP, d'une part, aux informations d'un titulaire d'un compte sur le site web doctissimo.fr, d'autre part.

55. La formation restreinte considère, dès lors, qu'en disposant de telles informations sur les personnes ayant répondu aux tests, la société traite des données de santé au sens de l'article 4-15 du RGPD.

56. En deuxième lieu, en l'absence d'autres conditions mobilisables pour permettre ledit traitement au cas d'espèce au titre de l'article 9-2-b) à j) du RGPD, la formation restreinte considère qu'un tel traitement ne peut être mis en œuvre que sur la base du consentement explicite de la personne concernée, au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques, en application de l'article 9-2-a) du RGPD. La formation restreinte rappelle que le caractère explicite du consentement s'analyse au cas par cas et dépend du contexte du traitement des données de santé. Lorsque le service demandé par l'utilisateur implique nécessairement le traitement de données de santé, il est cependant nécessaire que l'utilisateur ait pleinement conscience de ce que ses données de santé seront traitées et parfois conservés par le responsable de traitement, ce qui implique en principe une information explicite sur ce point lors du recueil du consentement.

57. La formation restreinte relève que, jusqu'au retrait du site web des tests susceptibles d'engendrer la collecte de données de santé le 12 septembre 2020, aucun avertissement particulier ni mécanisme de recueil du consentement ne figurait sur les questionnaires afin de s'assurer que la personne avait conscience et consentait au traitement de ses données de santé.

58. La formation restreinte rappelle qu'elle a déjà adopté des mesures correctrices à l'encontre de responsables de traitement ne recueillant pas le consentement exprès des personnes à la collecte et au traitement de leurs données sensibles, notamment dans ses délibérations n° 2016-405 du 15 décembre 2016 et n° 2016-406 du 15 décembre 2016.

59. En troisième lieu, la formation restreinte relève que le refus d'accompagnement de la CNIL, matérialisé par le courrier de la direction de l'accompagnement juridique de la Commission du 30 avril 2021 en réponse à la demande de la société du 8 avril 2021, s'inscrit dans le cadre prévu par la charte d'accompagnement des professionnels de la CNIL, qui prévoit une impossibilité d'accompagner les organismes dans leur mise en conformité lorsqu'une procédure de contrôle est en cours. La formation restreinte relève que si la CNIL peut répondre à une demande de conseil à l'issue du contrôle si la phase répressive n'est pas engagée, tel n'est pas le cas en l'espèce puisqu'une procédure de sanction a postérieurement été engagée.

60. En quatrième lieu, la formation restreinte relève que selon la société, la part des tests proposés sur le site internet de DOCTISSIMO concernée par la collecte des données de santé est de l'ordre de 5%. La formation restreinte note, en conséquence, que ledit traitement de données sensibles concerne environ […] réponses.

61. En conséquence, la formation restreinte considère que les faits précités constituent un manquement aux obligations de l'article 9 du RGPD dès lors que, jusqu'au 12 septembre 2020 les données étaient traitées en méconnaissance des conditions définies par cet article.

62. La formation restreinte relève enfin que les tests susceptibles d'engendrer la collecte des données de santé sont de nouveau accessibles depuis le 15 octobre 2020 et que la participation à ces tests est conditionnée au fait que les internautes consentent, au moyen d'une case à cocher, au traitement de leurs informations. Elle relève que la société s'est mise en conformité au cours de la procédure de contrôle, ce qui ne remet toutefois pas en cause l'existence du manquement pour les faits passés.

D. Sur le manquement à l'obligation d'information des personnes en application de l'article 13 du RGPD

63. Aux termes de l'article 13 du RGPD, le responsable du traitement doit fournir à la personne concernée par le traitement plusieurs informations au moment où les données sont obtenues.

64. Dans son rapport initial la rapporteure relevait que l'information fournie par la société sur le site web www.doctissimo.fr ne précisait pas la base juridique des traitements mis en œuvre. La rapporteure relevait également qu'aucune mention ne précisait si la fourniture d'une information était obligatoire en ce qu'elle avait un caractère

réglementaire ou contractuel ou si elle conditionnait la conclusion d'un contrat et si la personne concernée était tenue de fournir les données à caractère personnel.

65. En défense, la société communique sa " Politique de protection des données " et indique qu'elle contient les références aux bases légales applicables.

66. Lors de la séance, compte tenu des éléments communiqués par la société dans le cadre de l'instruction, la rapporteure a proposé à la formation restreinte de ne pas retenir le manquement en lien avec l'information fournie par la société sur le site web, considérant que la " Politique de protection des données " accessible depuis le site web www.doctissimo.fr, contient les informations sur la base juridique appliquée pour les traitements mis en œuvre et le fait que certaines informations conditionnent la création d'un compte utilisateur ou ont un caractère réglementaire.

67. La formation restreinte considère que le manquement à l'article 13 du RGPD n'est pas constitué.

E. Sur le manquement à l'obligation d'encadrer par un acte juridique formalisé les traitements effectués conjointement avec un autre responsable de traitement en application de l'article 26 du RGPD

68. Aux termes de l'article 26 du RGPD, " 1. Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis. Un point de contact pour les personnes concernées peut être désigné dans l'accord.

2. L'accord visé au paragraphe 1 reflète dûment les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées. Les grandes lignes de l'accord sont mises à la disposition de la personne concernée.

3. Indépendamment des termes de l'accord visé au paragraphe 1, la personne concernée peut exercer les droits que lui confère le présent règlement à l'égard de et contre chacun des responsables du traitement ".

69. La rapporteure relève qu'il ressort des éléments transmis par la société DOCTISSIMO qu'elle se considère responsable conjoint de [...]et de [...]. Or, la rapporteure relève qu'aucun contrat conclu entre la société et ces deux entités ne contient de disposition relative à la définition des obligations respectives des parties en application de l'article 26 du RGPD. La rapporteure note néanmoins que la société a transmis, le 24 février 2021, des avenants aux contrats existants qui définissent les obligations respectives des parties.

70. En défense, la société ne remet pas en cause la réalité du manquement allégué mais soutient qu'aucune personne concernée ne s'est plainte de ne pas avoir reçu les informations nécessaires ou que ses droits n'aient été respectés et qu'ainsi l'exercice des droits des personnes était garanti. En conséquence, la société soutient que ce manquement doit être écarté.

71. La formation restreinte relève qu'il ressort des éléments transmis par la société DOCTISSIMO que cette dernière est responsable conjointe avec les sociétés [...], d'une part, s'agissant des traitements liés à la commercialisation des espaces publicitaire du site web www.doctissimo.fr et [...], d'autre part, au sujet des traitements de données ayant recours aux outils techniques et aux structures fonctionnelles mises à disposition par cette dernière.

72. Si les éléments transmis par la société DOCTISSIMO attestent que des avenants relatifs à la protection des données à caractère personnel, définissant les obligations respectives des parties, ont été conclus depuis le 24 février 2021, conformément aux exigences de l'article 26 du RGPD, la formation restreinte note que la relation de responsabilité conjointe n'était pas encadrée au moment des contrôles de la CNIL.

73. Dès lors, au regard de ce qui précède, la formation restreinte considère que les faits précités constituent un manquement à l'article 26 du RGPD, l'absence de plainte ou de préjudice pour les utilisateurs étant inopérante. La formation restreinte note les mesures de mises en conformité effectuées au cours de la procédure, lesquelles ne sauraient exonérer la société de sa responsabilité pour le manquement constaté.

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

74. 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 ; […] ".

a. Sur l'absence de sécurité relative à la navigation des utilisateurs sur le site web

75. La rapporteure relève que lors du contrôle sur place du 1er octobre 2020, la société a indiqué à la délégation qu'avant octobre 2019, les pages relatives aux tests mis en œuvre sur le site web www.doctissimo.fr par la société [...], utilisaient par

défaut le protocole de communication " HTTP ". La rapporteure relève, dès lors, que ce protocole de communication était présent sur les pages de tests à partir desquelles des données à caractère personnel – comprenant des données de santé – étaient renseignées par des utilisateurs.

76. La rapporteure relève néanmoins que la délégation a constaté le 9 septembre 2020 que lesdites pages utilisaient désormais le protocole de communication " HTTPS ".

77. En défense, la société soutient que le RGPD ne prévoit pas d'obligation de mettre en œuvre le protocole HTTPS et que la CNIL ne peut donc sanctionner l'usage du protocole " http " sur la base d'une simple recommandation alors même qu'il n'a fait l'objet d'aucune violation de données. La société précise également que l'absence de protocole " HTTPS " avant octobre 2019 était la pratique dominante du marché et conforme à " l'état de l'art " en la matière. Enfin, la société soutient que la délégation de la CNIL n'a pas pu constater les faits puisque le manquement est fondé uniquement sur des déclarations de salariés de la société qui ne sauraient être utilisées pour fonder une sanction, sauf à méconnaître le droit de DOCTISSIMO à ne pas s'auto-incriminer.

78. En premier lieu, la formation restreinte rappelle que, en application de l'article 32 du RGPD, il incombe au responsable de traitement de prendre des " mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ".

79. La formation restreinte estime tout d'abord que la survenance d'une violation de données n'est pas nécessaire à la caractérisation d'un manquement et qu'elle a adopté à plusieurs reprises des sanctions pécuniaires dans lesquelles la constitution d'un manquement à l'article 32 RGPD est fondé sur l'absence de mesures suffisantes pour garantir la sécurité des données à caractère personnel, notamment dans les délibérations n° SAN-2019-006 du 13 juin 2019 et n° SAN-2021-021 du 28 décembre 2021 à l'encontre de la société […].

80. En l'espèce, la formation restreinte relève que le protocole " HTTP " est un protocole de communication qui ne permet ni l'authentification du site web, ni le chiffrement des données lors de leur transmission vers les serveurs de la société [...], ce qui ne permet pas de garantir l'authenticité du site consulté, ni l'intégrité et la confidentialité des données échangées, exposant les données à caractère personnel traitées par le biais de ces pages à des risques d'écoute, d'interception ou de modification à l'insu de l'utilisateur, ce qui peut conduire à porter atteinte à la vie privée des personnes concernées.

81. La formation restreinte relève à titre d'éclairage que la nécessité d'assurer la confidentialité des canaux de transmission de données à caractère personnel est soulignée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) depuis 2013 notamment dans sa " Recommandations pour la mise en œuvre d'un site web : maîtriser les standards de sécurité côté navigateur " qui précise que " La mise en place de HTTPS sur un site ou une application web est une garantie de sécurité qui repose sur TLS pour assurer la confidentialité et l'intégrité des informations échangées, ainsi que l'authenticité du serveur contacté. L'absence de cette garantie peut entraîner de nombreux abus sans pour autant que l'intention soit malveillante ".

82. La formation restreinte relève également que la Commission recommande de façon constante depuis la publication de son guide " La sécurité des données personnelles " en 2018, de mettre en œuvre, à titre de précautions élémentaires, le protocole " TLS " en utilisant uniquement les versions les plus récentes et en vérifiant sa bonne mise en œuvre.

83. La formation restreinte considère que si les recommandations de l'ANSSI et le guide de la CNIL n'ont pas un caractère impératif, ils sont mobilisés à titre d'éclairage et exposent néanmoins les précautions élémentaires de sécurité correspondant à l'état de l'art. La formation restreinte considère en conséquence, que l'usage du protocole " HTTPS " relevait de l'état de l'art avant le mois d'octobre 2019, contrairement à ce que soutient la société.

84. La formation restreinte relève en outre que les données à caractère personnel en question sont des données sensibles puisqu'il s'agit des réponses des utilisateurs à des tests impliquant la collecte de données concernant leur santé associées à leur adresse IP. Dès lors, la prise en compte de ces risques pour la protection des données à caractère personnel et de la vie privée des personnes conduit la formation restreinte à considérer que les mesures déployées pour garantir la sécurité des données, en l'espèce, étaient insuffisantes dès lors que des données à caractère personnel transitaient vers les serveurs de la société [...].

85. En conséquence, la formation restreinte considère, au regard des données personnelles objet du traitement, que l'absence de mise en place de la mesure de sécurité de base que constitue l'utilisation du protocole " HTTPS " ou d'une autre mesure de sécurité équivalente caractérise un manquement à l'article 32 du RGPD. La formation restreinte relève néanmoins que la délégation a constaté lors de son contrôle du 9 septembre 2020 que les pages relatives aux tests mis en œuvre sur le site web www.doctissimo.fr utilisaient le protocole de communication " HTTPS ". Elle rappelle néanmoins que les mesures de mises en conformité effectuées ne sauraient exonérer la société de sa responsabilité pour le manquement constaté.

86. En second lieu, la formation restreinte rappelle que si le droit pour une personne de ne pas participer à sa propre incrimination implique que l'accusation ne peut fonder son argumentation en recourant à des éléments de preuve obtenus par la contrainte ou les pressions, elle considère que l'ensemble des informations recueillies par la CNIL l'ont été dans le cadre de la procédure de contrôle fondée sur l'article 19 de la loi Informatique et Libertés. La formation restreinte relève que la société a été mise en mesure d'émettre des observations à l'issue de la rédaction du procès-verbal mais également de contester l'analyse faite de ces déclarations. Or, la formation restreinte relève que la société ne conteste pas avoir eu recours jusqu'en octobre 2019 au protocole " HTTP ". Enfin, la formation restreinte note que le conseil de la société, [...], était présent lors du contrôle sur place réalisé le 1er octobre 2020 par la CNIL. La formation restreinte considère qu'il n'y a pas eu de contrainte contraire à l'article 6 de la Convention européenne des droits de l'homme lorsque les salariés de la société DOCTISSIMO ont volontairement fait des déclarations concernant l'utilisation du protocole " HTTP " au cours de la procédure de contrôle.

87. En conséquence, dès lors que la société DOCTISSIMO a méconnu une mesure de sécurité élémentaire et fait encourir des risques pour la sécurité des données à caractère personnel de ses utilisateurs jusqu'en octobre 2019, la formation

restreinte considère que les faits précités constituent un manquement aux obligations de l'article 32 du RGPD pour les faits passés.

b. Sur l'absence de sécurité relative au stockage des mots de passe des utilisateurs du site web

88. La rapporteure relève que la délégation a constaté que la société conserve les mots de passe des utilisateurs du site web dans un format obtenu par un procédé en trois étapes : les mots de passe sont transformés une première fois à l'aide de l'algorithme de hachage MD5, ensuite le résultat obtenu est transformé une seconde fois via la fonction " password_hash " du langage de programmation PHP utilisée par défaut avec l'algorithme Bcrypt et enfin, le résultat obtenu est stocké dans la base de données de la société. La rapporteure considère que ces modalités de stockage des mots de passe sont insuffisantes pour assurer la sécurité des données à caractère personnel auxquelles ils permettent d'accéder (espace personnel contenant notamment les nom, prénom, date de naissance, adresse électronique et sexe de la personne concernée).

89. En défense, la société reconnaît que l'algorithme MD5 n'apporte pas les garanties suffisantes pour conserver des hash sécurisés de mot de passe, raison pour laquelle elle a décidé de le coupler avec la fonction Bcrypt. La société indique que cette technique permettrait de créer des mots de passe plus longs et donc plus robustes. Elle soutient que cette technique est toujours largement utilisée par les sites internet et qu'elle était considérée jusque très récemment comme une technique valable en matière de sécurité puisque ce n'est que depuis 2020 que certains chercheurs pointent les limites de cette méthode. En outre, la société indique qu'aucune attaque n'a été documentée et dès lors, que le risque élevé évoqué par la rapporteure est hypothétique et ne justifie pas le prononcé d'une sanction. Enfin, la société a indiqué avoir supprimé le pré-hachage depuis le 7 septembre 2022 ainsi que l'ensemble des mots de passe des utilisateurs qui devront à leur prochaine connexion, mettre à jour leur mot de passe. La société a précisé que les nouveaux mots de passe seront stockés selon les modalités de cette nouvelle méthode qui représente une fonction de chiffrement " non réversible et sûre ".

90. En premier 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.

91. La formation restreinte rappelle également à titre d'éclairage que depuis 2013, l'ANSSI précise 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 ".

92. La formation restreinte relève également que la Commission recommande dans sa délibération portant adoption d'une recommandation relative aux mots de passe, n° 2017-012 du 19 janvier 2017, " qu'il 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. ".

93. La formation restreinte considère que les recommandations de l'ANSSI et de la CNIL sont mobilisés à titre d'éclairage et exposent les précautions élémentaires de sécurité correspondant à l'état de l'art.

94. La formation restreinte rappelle que si elle est techniquement possible, la combinaison d'algorithme cryptographique pour assurer le stockage de données à caractère personnel n'est pas recommandée.

95. La formation restreinte relève, en l'espèce, que l'algorithme MD5 n'est plus considéré comme à l'état de l'art depuis 2004 et que son utilisation en cryptographie ou en sécurité est proscrite. Elle rappelle que l'ANSSI l'a ensuite retiré du référentiel général de sécurité dès 2014, rappelant que l'algorithme MD5 était considéré comme " définitivement cassé ".

96. La formation restreinte considère également que le procédé consistant à transformer préalablement le mot de passe au moyen de la fonction MD5 introduit ensuite une vulnérabilité dans la fonction Bcrypt. Elle rappelle que l'Open Web Application Security Project (OWASP) déconseille cette pratique car elle introduit un risque de forme particulière d'attaque par bourrage d'identifiants dès lors que la fonction Bcrypt est combinée avec une autre fonction, telles que la fonction MD5. La formation restreinte relève qu'une telle configuration expose les données à un risque d'attaque basée sur la réutilisation des couples MD5 et mots de passe issus de bases de données fuitées.

97. Dès lors, la formation restreinte considère que la politique de gestion des mots de passe de la société ne mobilise pas de mesures satisfaisantes pour assurer la sécurité des données à caractère personnel auxquelles ils permettent d'accéder.

98. En second lieu, la formation restreinte rappelle que la survenance d'une attaque ou d'une violation de données n'est pas nécessaire à la caractérisation d'un manquement à l'article 32 du RGPD.

99. En conséquence, la formation restreinte considère que les faits précités constituent un manquement à l'article 32 du RGPD. Elle relève néanmoins que la société DOCTISSIMO a indiqué avoir mis en œuvre une nouvelle méthode de stockage des mots de passe à l'aide d'une fonction de chiffrement non réversible et sûre depuis le 7 septembre 2022, de sorte qu'il n'y a pas lieu à adresser d'injonction à la société sur ce point. La formation restreinte rappelle cependant que les mesures de mises en conformité effectuées ne sauraient exonérer la société de sa responsabilité pour le passé.

G. Sur le manquement aux obligations de l'article 82 de la loi Informatique et Libertés

100. Aux termes de l'article 82 de la loi Informatique et Libertés, transposant l'article 5, paragraphe 3, de la directive " ePrivacy ", il est prévu que : " tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant :

1° De la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ;

2° Des moyens dont il dispose pour s'y opposer.

Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son consentement qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle.

Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :

1° Soit, a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;

2° Soit, est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur ".

a. Sur le dépôt de cookie sur le terminal de l'utilisateur sans recueil de son consentement

101. La rapporteure relève que lors du contrôle en ligne du 1er décembre 2020, la délégation a constaté lors de deux sessions de navigation différentes, à partir d'un historique de navigation vierge et avant toute action de sa part, que deux cookies étaient déposés sur son terminal dès son arrivée sur la page d'accueil du site web www.doctissimo.fr. La rapporteure relève que la société a indiqué que l'un de ces cookies, le cookie dénommé " af_session " avait pour finalité la diffusion de publicité ciblée.

102. En défense, la société ne conteste pas les faits décrits par la rapporteure. Elle soutient néanmoins que le dépôt du cookie publicitaire avant toute action de l'utilisateur découlait de sa double finalité, technique et publicitaire et indique avoir finalisé sa mise en conformité dès le 21 décembre 2020. Au cours des échanges, elle démontre par la communication d'un procès-verbal d'huissier, qu'à compter du 29 août 2022, aucun cookie autre que strictement technique n'est plus déposé sur le terminal des utilisateurs avant que leur consentement ne soit recueilli.

103. La formation restreinte rappelle que l'article 82 de loi Informatique et Libertés prévoit expressément que les opérations d'accès ou d'inscription d'informations dans le terminal d'un utilisateur ne peuvent avoir lieu qu'après que ce dernier ait exprimé son consentement, seuls les cookies ayant pour finalité exclusive de permettre ou de faciliter la communication par voie électronique, ou les cookies étant strictement nécessaires à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur, étant exemptés de cette obligation.

104. La formation restreinte considère que les cookies publicitaires, n'ayant pas pour finalité exclusive de permettre ou faciliter la communication par voie électronique et n'étant pas strictement nécessaires à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur, ne peuvent être déposés ou lus sur le terminal de la personne, conformément à l'article 82 de la loi Informatique et Libertés, tant qu'elle n'a pas fourni son consentement.

105. En conséquence, la formation restreinte considère qu'en permettant le dépôt et la lecture du cookie " af session " sur le terminal des personnes lors de leur arrivée sur le site doctissimo.fr, sans recueillir préalablement leur consentement, alors qu'il a pour finalité la diffusion de publicité ciblée, la société a privé celles-ci de la possibilité qui leur a été attribuée par l'article 82 de la loi Informatique et Libertés, d'exercer un choix quant au dépôt de traceurs sur leur équipement terminal. La formation restreinte relève que plusieurs millions de personnes ont été concernées, la société revendiquant environ 276 millions de visiteurs uniques du site web doctissimo.fr entre le mois de février 2020 et de février 2021

106. La formation restreinte relève que la société DOCTISSIMO a démontré au cours de la procédure, qu'à compter du 29 août 2022 aucun cookie autre que strictement technique n'est plus déposé sur le terminal des utilisateurs avant que leur consentement ne soit recueilli, de sorte qu'il n'y a pas lieu à adresser d'injonction à la société sur ce point. Elle rappelle néanmoins que les mesures de mises en conformité effectuées ne sauraient exonérer la société de sa responsabilité pour le passé.

b. Sur l'insuffisance du mécanisme proposé aux utilisateurs pour refuser le dépôt de cookies

107. La rapporteure relève que la délégation a constaté, lors du contrôle en ligne du 1er décembre 2020, la présence d'un mécanisme permettant aux utilisateurs de " paramétrer les cookies " (mécanisme dit de " Consent Management Platform ", ci-après CMP). Lors de ce contrôle, la délégation a cliqué sur la case intitulée " REFUSER TOUT ", situé en bas à droite de la CMP s'affichant sur le site. Cependant, la rapporteure a relevé que le cookie à finalité publicitaire " af_session ", qui avait déjà été déposé, demeurait stocké sur l'équipement terminal de l'utilisateur. Ensuite, la rapporteure a relevé qu'après avoir navigué vers une autre page du site pour consulter un article en ligne, la délégation a relevé que le même cookie " af_session " précédemment déposé, demeurait stocké sur l'équipement terminal de l'utilisateur. Enfin, la rapporteure a également relevé que la délégation a constaté le dépôt sur l'équipement terminal de l'utilisateur de deux nouveaux cookies ayant pour finalité la diffusion de publicité ciblée dénommés " UID " et " GED_PLAYLIST_ACTIVITY ", respectivement déposés par des tiers, les partenaires […], sous les noms de domaine " .scorecardresearch.com " et " www.doctissimo.fr ", malgré le refus exprimé par l'utilisateur.

108. En défense, la société ne conteste pas les faits décrits par la rapporteure. Néanmoins, la société rappelle le contexte particulier dans lequel le contrôle en ligne est intervenu puisque la CNIL avait publié le 17 septembre 2020 ses nouvelles lignes directrices concernant les cookies qui ont eu d'importantes conséquences sur les outils de collecte du consentement et de refus des cookies. En outre, la société soutient que des dysfonctionnements techniques non-intentionnels ont engendré le dépôt des deux cookies publicitaires après refus de la délégation et produit un échange extrait d'un forum Google Groups datant de janvier 2021 dans lequel un éditeur d'un site internet fait remonter un dysfonctionnement aux services de Google relatif au cookie dénommé " GED_PLAYLIST_ACTIVITY ". Elle soutient en conséquence que le manquement est non-intentionnel. Enfin, la société démontre par la communication du procès-verbal d'huissier précité, qu'à compter du 29 août 2022, en cas de refus de l'utilisateur aucun cookie autre que strictement technique n'est plus déposé sur son terminal.

109. En premier lieu, la formation restreinte relève d'abord que des opérations de lecture et / ou d'écriture d'informations dans l'équipement terminal de communications électroniques de l'utilisateur ont lieu après qu'il a exprimé son refus au dépôt et à la lecture de cookies à finalité publicitaire et navigué vers une autre page du site web. La formation restreinte considère que les moyens fournis aux personnes pour leur permettre de refuser toute action tendant à accéder à des informations déjà stockées dans leur équipement terminal ou à inscrire des informations dans cet équipement sont ineffectifs.

110. Ensuite, la formation restreinte considère que la société DOCTISSIMO, en tant qu'elle édite le site web doctissimo.fr, a une part de responsabilité dans le respect des obligations de l'article 82 de la loi Informatique et Libertés pour les opérations de lecture et / ou d'écriture d'informations effectuées dans le terminal des utilisateurs lors de la visite de son site web, y compris celles réalisées par des tiers qui sont ses partenaires commerciaux. La formation restreinte rappelle que le Conseil d'Etat a jugé qu'au titre des obligations qui pèsent sur l'éditeur de site, figurent celle de s'assurer auprès de ses partenaires, d'une part, qu'ils n'émettent pas, par l'intermédiaire de son site, des traceurs qui ne respectent pas la règlementation applicable en France et, d'autre part, celle d'effectuer toute démarche utile auprès d'eux pour mettre fin à des manquements (CE, 6 juin 2018, Editions Croque Futur, n°412589). La formation restreinte rappelle qu'elle a déjà sanctionné un manquement à l'article 82 de la loi précitée en lien avec des opérations de lecture et / ou d'écriture d'informations effectuées par des tiers dans le terminal des utilisateurs dans la délibération n° SAN-2021-013 du 27 juillet 2021 à l'encontre de la […].

111. En deuxième lieu, la formation restreinte rappelle que la CNIL a mis en œuvre un plan de mise en conformité sur la question des cookies étalé sur plusieurs années et qu'elle a particulièrement communiqué sur ces évolutions, notamment dès 2019 sur son site web, ou encore le 1er octobre 2020 à l'occasion de la publication des lignes directrices et de la recommandation du 17 septembre 2020. La mise en conformité devait avoir eu lieu pour le 1er avril 2021 et des centaines de milliers d'acteurs, des plus petits sites aux plus importants, se sont mis en conformité et ont introduit sur leur interface de recueil du consentement un bouton " Refuser " ou " Continuer sans accepter ". La formation restreinte relève que les manquements constatés lors du contrôle en ligne du 1er décembre 2020, qui portent sur le dépôt de cookies sur le terminal de l'utilisateur sans son consentement et avant toute action ainsi qu'après qu'il ait cliqué sur le bouton " TOUT REFUSER ", étaient des pratiques identifiées par la CNIL comme étant contraires à l'article 82 de la loi Informatique et Libertés dès 2013. Elle considère que le contexte de publication par la CNIL de ses nouvelles lignes directrices concernant les cookies, dans lequel s'inscrit le contrôle du 1er décembre 2020 ne permet donc pas d'atténuer la portée des manquements relevés et que la société se devait d'être à la fois particulièrement vigilante quant au respect de ses obligations en matière de cookies et également attentive aux évolutions de la réglementation en la matière, notamment à la suite du renforcement des conditions du consentement consécutif à l'entrée en application du RGPD.

112. En troisième lieu, au regard des échanges et des pièces communiquées dans le cadre de l'instruction, la formation restreinte considère que les dysfonctionnements invoqués par la société ne permettent pas de minimiser sa responsabilité en ce qu'ils sont postérieurs au contrôle de la CNIL et concernent un autre éditeur de site internet. La formation restreinte considère, en tout état de cause, qu'il revenait à DOCTISSIMO de s'assurer du respect des obligations de l'article 82 de la loi Informatique et Libertés et ainsi de s'assurer auprès de ses partenaires qu'ils n'émettaient pas, par l'intermédiaire de son site, des traceurs qui ne respectent pas la règlementation applicable en France et d'effectuer toute démarche utile auprès d'eux pour mettre fin à des manquements, ce que la société n'a fait qu'après le contrôle de la CNIL du 1er décembre 2020.

113. En conséquence, il résulte de l'ensemble de ces éléments qu'en déposant des cookies soumis à consentement sur le terminal de l'utilisateur avant toute action de sa part et en privant d'effet le refus du dépôt et de la lecture des cookies à finalité publicitaire, la société DOCTISSIMO a méconnu les dispositions de l'article 82 de la loi Informatique et Libertés.

114. La formation restreinte relève que la société DOCTISSIMO a démontré au cours de la procédure, qu'à compter du 29 août 2022 aucun cookie autre que strictement technique n'est déposé sur le terminal des utilisateurs avant que leur consentement ne soit recueilli, ni en cas de refus des utilisateurs, de sorte qu'il n'y a pas lieu à adresser d'injonction à la société sur ce point. Elle rappelle néanmoins que les mesures de mises en conformité effectuées ne sauraient exonérer la société de responsabilité pour le passé.

III. Sur les mesures correctrices et leur publicité

115. 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. "

116. 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.

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

a. Sur le prononcé d'une amende administrative

117. La société considère que l'amende administrative proposée est disproportionnée par rapport aux manquement allégués portant sur des faits anciens et à sa conduite puisqu'elle a mis en œuvre les mesures de remédiation nécessaires.

118. 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 certain cas, le niveau de dommage subi par les personnes.

119. La formation restreinte relève d'abord le nombre et l'étendue des manquements reprochés à la société, au nombre de cinq dont quatre manquements au RGPD.

120. S'agissant du manquement au principe de limitation de la durée de conservation des données à caractère personnel, la société a fait preuve d'une négligence en conservant les données relatives aux tests réalisés par les utilisateurs du site web www.doctissimo.fr pour une durée excédant les finalités pour lesquelles elles étaient traitées. La formation restreinte note, toutefois, qu'il s'agit d'un manquement résultant du non-respect par le sous-traitant de ses propres obligations contractuelles et que la société DOCTISSIMO a rompu tout lien contractuelle avec celui-ci. Concernant les durées de conservation des comptes créés par les utilisateurs du site web, la formation restreinte rappelle que les mesures prises par la société ne permettaient pas d'anonymiser les données à caractère personnel de l'utilisateur dont le compte était inactif depuis plus de trois ans. Elle relève que ce manquement concerne un nombre important de personnes, la société revendiquant environ […] utilisateurs disposant d'un compte créé à partir du site web et […] utilisateurs ayant répondu à une question d'un test ayant pour thème la santé.

121. S'agissant du manquement à l'obligation de recueillir le consentement des personnes concernées au traitement de données sensibles relatives à la santé, la formation restreinte relève tout d'abord que la société a fait preuve de négligence en s'abstenant de recueillir le consentement des utilisateurs lorsqu'elle leur proposait des tests supposant la collecte de données relatives à leur santé. Elle relève ensuite que ce manquement concerne un nombre important de personnes, la société indiquant que 5% des tests proposés seraient susceptibles de permettre la collecte des données de santé, ce qui représente environ […] réponses. La formation restreinte considère par ailleurs qu'il convient, concernant ce manquement, de prendre en compte la nature de l'acteur concerné et son secteur d'activité. En effet, la société DOCTISSIMO diffusant des contenus numériques relatifs à la santé, elle ne saurait éluder une telle obligation.

122. S'agissant du manquement à l'obligation d'assurer la sécurité des données personnelles, la formation restreinte considère qu'il a contribué à accentuer le fait que les données à caractère personnel des personnes traitées dans ce cadre n'aient pas bénéficié de la protection offerte par le RGPD.

123. S'agissant du manquement relatif aux cookies déposés sur le terminal de l'utilisateur lors de la visite du site web de la société, la formation restreinte considère que l'absence de recueil du consentement a concerné chacune des personnes qui ont visité le site web en question, soit nécessairement plusieurs millions de personnes, compte tenu du fait que la société revendique environ […] de visiteurs uniques du site web doctissimo.fr entre les mois de février 2020 et février 2021.

124. Enfin, la formation restreinte relève que les mesures de conformité mises en place à la suite de la notification du rapport de sanction n'exonèrent par la société de sa responsabilité pour les manquements constatés.

125. En conséquence, la formation restreinte considère qu'il y a lieu de prononcer une amende administrative au regard des manquements constitués aux article 5- 1-e), 9-2, 26 et 32 du RGPD et au regard du manquement constitué à l'article 82 de la loi Informatique et Libertés.

b. Sur le montant de l'amende administrative

126. La formation restreinte relève d'abord que les manquements relatifs aux articles 5-1-e) et 9-2 du RGPD sont des manquements à des principes clé 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 et jusqu'à 4 % du chiffre d'affaires annuel, le montant le plus élevé étant retenu.

127. La formation restreinte rappelle ensuite que les amendes administratives doivent être à la fois dissuasives et proportionnées. La formation restreinte relève que la société DOCTISSIMO a réalisé, en 2021, un chiffre d'affaires d'environ […] pour un résultat net négatif de […].

128. La formation restreinte relève que la société DOCTISSIMO est détenue à 100 % par la société par actions simplifiée unipersonnelle UNIFY, qui est elle-même détenue par le groupe REWORLD MEDIA. Ce dernier a réalisé en 2021 un chiffre d'affaires consolidé d'environ 496,8 millions d'euros et un résultat net en progression de 42,2 millions d'euros.

129. Dès lors, au regard de la responsabilité de la société, de ses capacités financières et des critères pertinents de l'article 83 du Règlement évoqués ci-avant, la formation restreinte estime qu'une amende administrative d'un montant de deux cent quatre-vingt mille euros, au regard des manquements constitués aux articles 5-1-e), 9-2, 26 et 32 du RGPD et qu'une amende administrative d'un montant de cent mille euros au regard des manquements constitués à l'article 82 de la loi Informatique et Libertés apparaissent justifiées.

B. Sur la publicité

130. La société conteste la proposition de la rapporteure de rendre publique la présente décision. Elle considère qu'au vu de l'ancienneté des faits et de la mise en conformité de la société, la vertu pédagogique et informative de la mesure de publicité de la sanction n'existe plus. Pour justifier cette demande de publicité, la rapporteure invoque notamment le nombre de personnes concernées et l'ancienneté de certaines données.

131. 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. La formation restreinte considère également que la publicité de la sanction permettra notamment d'informer l'ensemble des personnes concernées des suites apportées aux manquements.

132. 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 DOCTISSIMO une amende administrative d'un montant de deux cent quatre-vingt mille euros (280 000 €) au regard des manquements constitués aux articles 5-1-e), 9-2, 26 et 32 du règlement (UE) n° 2016/679 du 27 avril 2016 relatif à la protection des données ;

• prononcer à l'encontre de la société DOCTISSIMO une amende administrative d'un montant de cent mille euros (100 000 €) au regard du manquement constitué à l'article 82 de la loi du 6 janvier 1978 modifiée ;

• 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 vice-président

Philippe-Pierre CABOURDIN

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.