Délibération de la formation restreinte CNIL n° SAN – 2019-005 du 28 mai 2019 prononçant une sanction pécuniaire à l'encontre de la société SERGIC

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 Sylvie LEMMET et Mme Christine MAUGÜE, membres ;

Vu la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

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 loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 45 et suivants ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2018-186C du 5 septembre 2018 de la Présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification ;

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 1 er février 2019;

Vu le rapport de M. Éric PÉRÈS, commissaire rapporteur, du 4 février 2019 ;

Vu les observations écrites versées par la société SERGIC le 4 mars 2019 ;

Vu les observations en réponse du commissaire rapporteur du 15 mars 2019 ;

Vu les observations en réponse versées par la société SERGIC le 2 avril 2019 ainsi que les observations orales formulées lors de la séance de la formation restreinte ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 11 avril 2019 :

M. Éric PÉRÈS, commissaire, entendu en son rapport ;

En qualité de représentants de la société SERGIC : […]

La société ayant eu la parole en dernier ;

Après en avoir délibéré, a adopté la décision suivante :

1.La société SERGIC (ci-après la société) est spécialisée dans la promotion immobilière, l'achat, la vente, la location et la gestion immobilière. Elle emploie 486 personnes et a réalisé en 2017 un chiffre d'affaires d'environ 43 millions d'euros.

2.Pour les besoins de son activité, la société édite le site web www.sergic.com (ci-après le site) qui permet notamment aux candidats à la location d'un bien de télécharger les pièces justificatives nécessaires à la constitution de leur dossier.

3.Le 12 août 2018, la Commission nationale de l'informatique et des libertés (ci-après CNIL ou la Commission) a été saisie d'une plainte d'un utilisateur du site. Le plaignant indiquait qu'une modification du caractère X dans l'adresse URL composée comme suit : https://www.crm.sergic.com/documents/upload/eresa/X.pdf , où X représente un nombre entier, lui avait permis d'accéder aux pièces justificatives qu'il avait lui-même téléchargées via le site mais également à celles téléchargées par d'autres candidats à la location. Dans sa plainte, le plaignant a fourni plusieurs exemples d' adresses URL à partir desquelles il a pu accéder à des pièces téléchargées par des tiers. Il a indiqué avoir informé la société de ces faits dès le mois de mars 2018.

4.En application de la décision n° 2018-186C du 5 septembre 2018 de la Présidente de la Commission, une mission de contrôle en ligne puis une mission de contrôle au sein des locaux de la société ont été effectuées respectivement les 7 et 13 septembre 2018. Ces missions ont eu pour objet de vérifier la conformité à la loi du 6 janvier 1978 modifiée (ci-après la loi

Informatique et Libertés) et au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après RGPD ou le Règlement) des traitements de données à caractère personnel accessibles à partir du domaine sergic.com ou portant sur des données à caractère personnel collectées à partir de ce dernier.

5.Au cours de la mission de contrôle en ligne, la délégation a constaté que la saisie de l'une des adresses URL fournies par le plaignant permettait de télécharger un avis d'imposition établi à un nom différent du sien. La délégation a ensuite procédé au téléchargement de 9 446 documents au moyen d'un script, parmi lesquels des copies de cartes d'identité, de cartes Vitale, d'avis d'imposition, d'actes de décès, d'actes de mariage, d'attestations d'affiliation à la sécurité sociale, d'attestations délivrées par la caisse d'allocations familiales, d'attestations de pension d'invalidité, de jugements de divorce, de relevés de compte, de relevés d'identité bancaire et de quittances de loyers.

6.La société a été informée le 7 septembre, par la délégation, de l'existence d'un défaut de sécurité sur son site et un courrier électronique contenant le type d'adresses URL concernées par ce défaut de sécurité lui a été adressé.

7. Le 13 septembre 2018, au cours de la mission de contrôle dans les locaux de la société, la délégation de la CNIL a constaté que les adresses URL fournies par le plaignant dans sa saisine permettaient toujours d'accéder aux documents en question. La société a indiqué à la délégation que les pièces justificatives téléchargées par les candidats à la location sont enregistrées dans un répertoire dédié. Il a été précisé que l'ensemble du répertoire avait été rendu accessible par le défaut de sécurité. Il ressort des constatations effectuées que ce répertoire contenait 290 870 fichiers au jour du contrôle. La société a en outre indiqué que les documents fournis par les candidats ne faisaient l'objet d'aucune purge et qu'ils n'étaient pas réutilisés ultérieurement, les documents des candidats ayant accédé à la location étant déplacés dans un autre répertoire de la base de données.

8.La société a confirmé à la délégation qu'un signalement l'informant de ce que des documents étaient librement accessibles depuis le site, sans authentification préalable, lui était parvenu en mars 2018. Elle a précisé qu'à la suite de ce signalement, elle avait procédé à une première phase d'analyse du défaut de sécurité, qui a donné lieu à un plan d'action mis en œuvre à partir de juin 2018. Elle a également indiqué qu'une première action permettant de ne plus afficher les adresses URL telles qu'elles apparaissaient au moment de la violation avait été déployée quelques jours avant le contrôle du 13 septembre. La société a ensuite expliqué qu'une mesure mettant définitivement un terme au défaut de sécurité devait être mise en production le 17 septembre 2018. Les procès-verbaux des 7 et 13 septembre ont été notifiés à la société le 17 septembre.

9.Aux fins d'instruction de ces éléments, la Présidente de la CNIL a désigné, le 1 er février 2019, M. Éric PÉRÈS en qualité de rapporteur sur le fondement de l'article 47 de la loi du 6 janvier 1978. Par courrier du 1 er février 2019, la Présidente de la CNIL a informé la société de cette désignation.

10.A l’issue de son instruction, le rapporteur a fait notifier à la société SERGIC, le 5 février 2019, un rapport détaillant les manquements relatifs aux articles 5 et 32 du RGPD qu’il estimait constitués en l’espèce.

11.Ce rapport proposait à la formation restreinte de la CNIL de prononcer à l’encontre de la société SERGIC une sanction pécuniaire de 900 000 euros et qui serait rendue publique.

12.Etait également jointe au rapport une convocation à la séance de la formation restreinte du 11 avril 2019. La société disposait d’un délai d’un mois pour communiquer ses observations écrites. Le 11 février 2019, la société a formulé une demande pour que la séance se tienne à huis-clos. Il a été fait droit à cette demande par courrier du 22 février 2019 dans la mesure où certains éléments versés aux débats sont protégés par le secret des affaires, tel que prévu par l’article L 151-1 du code du commerce.

13.Le 4 mars 2019, la société a produit des observations écrites sur le rapport. Ces observations ont fait l’objet d’une réponse du rapporteur le 15 mars 2019. Le 2 avril 2019, la société a produit de nouvelles observations en réponse à celles du rapporteur.

14.L’ensemble des observations ont été réitérées oralement par la société et le rapporteur lors de la séance de la formation restreinte du 11 avril 2019.

II. Motifs de la décision

Sur la demande de nullité des constatations en ligne du 7 septembre 2018

15.La société fait valoir qu’au cours du contrôle en ligne du 7 septembre 2018, les agents de la CNIL ont procédé à l’extraction des fichiers accessibles depuis des adresses URL composées comme suit : https://www.crm.sergic.com/documents/upload/eresa/X.pdf alors que les dispositions de l’article 44 de la loi Informatique et Libertés n’autorisent les agents de la CNIL qu’à consulter des données librement accessibles ou rendues accessibles et qu’elles ne rendent, en aucun cas, possible le maintien dans un système de traitement automatisé de données en vue d’extraire des données en procédant au téléchargement de celles-ci.

16.La société demande en conséquence à la formation restreinte de prononcer la nullité des constations contenues dans le procès-verbal n° 2018-186/1 du 7 septembre 2018.

17.La formation restreinte rappelle qu’aux termes de l’alinéa 3 du III de l’article 44 de la loi Informatique et Libertés , les agents de la Commission peuvent notamment, à partir d'un service de communication au public en ligne, consulter les données librement accessibles ou

rendues accessibles, y compris par imprudence, par négligence ou par le fait d'un tiers, le cas échéant en accédant et en se maintenant dans des systèmes de traitement automatisé de données le temps nécessaire aux constatations ; ils peuvent retranscrire les données par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle .

18.En téléchargeant les fichiers à partir des adresses URL susmentionnées, les agents de la CNIL ont bien procédé à une retranscription des données et non pas à une extraction, dans la mesure où les fichiers n'ont pas été déplacés de la base de données de la société mais ont simplement été copiés. La formation restreinte considère qu'en téléchargeant les fichiers rendus librement accessibles par le défaut de sécurité, les agents de la CNIL ont agi dans le strict respect des dispositions de l'article 44 précité, qui n'énumère au demeurant pas limitativement les formes que peuvent prendre les retranscriptions des agents habilités.

19.En conséquence, la demande de nullité sera rejetée.

2. Sur l'utilisation d'éléments issus de la réponse de la société SERGIC ENTREPRISES

20.La société note que dans le rapport notifié le 5 février 2019, le rapporteur a indiqué avoir tenu compte d'informations qui avaient été transmises par sa filiale, la société SERGIC ENTREPRISES, personne morale distincte de la société SERGIC, dans le cadre d'une procédure de sanction préalablement ouverte à l'encontre de cette dernière. La société SERGIC fait valoir que ni le rapport, ni la réponse du rapporteur n'indiquent clairement quelles sont les informations fournies par la société SERGIC ENTREPRISES sur lesquelles le rapporteur s'est appuyé dans le cadre de la présente procédure. La société indique ainsi ne pas savoir de quelle manière le rapporteur a tenu compte de ces éléments dans l'élaboration de sa proposition. Elle demande dès lors à la formation restreinte de statuer sur la seule base des observations et pièces qu'elle a fournies et d'exclure les informations fournies par la société SERGIC ENTREPRISES.

21. La formation restreinte constate tout d'abord que, dans son rapport du 4 février 2019, le rapporteur a clairement fait état de ce qu'une première procédure de sanction avait été initiée à l'encontre de la société SERGIC ENTREPRISES mais que les investigations menées dans le cadre de cette procédure avaient révélé que SERGIC ENTREPRISES n'était pas le responsable de traitement auquel des manquements pouvaient être reprochés. La formation restreinte note qu'au demeurant, la procédure de sanction initiée à l'encontre de la société SERGIC ENTREPRISES a été close le 31 janvier 2019.

22.La formation restreinte relève ensuite que, dans sa réponse aux observations de la société, le rapporteur a indiqué que les éléments dont il avait tenu compte pour établir son rapport étaient les informations relatives au fait que SERGIC avait procédé à la notification de la violation de données aux personnes concernées, au fait que le nombre de personnes

concernées par la violation de données a été clarifié et au fait que les documents transmis par les candidats étaient conservés à des fins précontentieuses et contentieuses.

23.Elle considère que les indications données par le rapporteur permettaient à la société d'identifier sans ambiguïté les informations en question et les développements du rapport les comportant.

24.Enfin, la formation restreinte souligne que l'ensemble des informations sur lesquelles le rapporteur a fondé sa proposition de sanction, quelle qu'en soit la source, ont été portées à la connaissance de la société SERGIC dans le cadre de la procédure et soumises à un débat contradictoire. Ce faisant, la société a eu connaissance de la prise en compte de ces informations et a été mise en mesure de remettre en cause l'exactitude des faits développés dans le rapport et d'en contester leur portée.

25.En conséquence, il convient de rejeter la demande de la société de ne pas prendre en considération les éléments issus de la procédure suivie contre la société SERGIC ENTREPRISES.

3. Sur l'absence de mise en demeure préalable

26.La société argue que les manquements qui lui sont reprochés auraient pu être corrigés dans le cadre d'une mise en demeure. Elle estime donc que l'engagement immédiat d'une procédure de sanction, sans mise en demeure préalable, l'a privée de la possibilité de se mettre en conformité.

27.La formation restreinte relève qu'il résulte de la lettre même des dispositions du III de l'article 45 de la loi du 6 janvier 1978 modifiée, issues de la loi n° 2018-493 du 20 juin 2018 visant à mettre en conformité les dispositions législatives nationales avec celles du RGPD, que le prononcé d'une sanction n'est pas subordonné à l'adoption préalable d'une mise en demeure. La décision de désigner un rapporteur et de saisir la formation restreinte est un pouvoir appartenant au Président de la CNIL, qui dispose de l'opportunité des poursuites et peut donc déterminer , en fonction des circonstances de l'espèce, les suites à apporter à des investigations en clôturant par exemple un dossier, en prononçant une mise en demeure ou en saisissant la formation restreinte en vue du prononcé d'une ou plusieurs mesures correctrices.

4. Sur le manquement à l'obligation d'assurer la sécurité et la confidentialité des données à caractère personnel

a. Sur la caractérisation du manquement

28.L’article 32 (1) du Règlement dispose que : 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 :

la pseudonymisation et le chiffrement des données à caractère personnel ;

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

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 ;

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

29.L’article 32 (2) prévoit que : Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

30. Il appartient à la formation restreinte de déterminer si la société SERGIC a manqué à son obligation d’assurer la sécurité des données personnelles traitées et si, en particulier, la société a mis en œuvre des moyens permettant de garantir leur confidentialité, afin d’empêcher qu’elles soient accessibles à des tiers non autorisés, conformément à l’article 32 (1) ii précité.

31.La formation restreinte note tout d’abord que l’existence d’un défaut de sécurité sur le site www.sergic.com n’est pas contestée par la société. Elle constate que ce défaut de sécurité a rendu possible la violation de données à caractère personnel dans la mesure où il a permis à des tiers non autorisés d’accéder à ces données.

32.La formation restreinte rappelle que lorsqu’une requête visant à accéder à une ressource est adressée à un serveur, celui-ci doit préalablement s’assurer que l’émetteur de cette requête est autorisé à accéder aux informations demandées. En l’espèce, tant le plaignant que la délégation de contrôle ont pu librement consulter les documents transmis à la société par un grand nombre de candidats à la location, sans qu’une mesure ne restreigne cette possibilité.

33.Cet accès aux documents conservés par la société traduit une conception défectueuse du site, caractérisée en l’espèce par l’absence de mise en place d’une procédure d’authentification des utilisateurs. La violation de données résultant de ce défaut de sécurité aurait pu être évitée si, par exemple, la société avait mis en œuvre un moyen d’authentification permettant de s’assurer que les personnes accédant aux documents étaient bien celles à l’origine de leur téléchargement sur le répertoire en question, et que seules celles-ci pouvaient y accéder. La mise en place d’une telle fonctionnalité constitue une

précaution d'usage essentielle, qui aurait permis de garantir la confidentialité des données personnelles traitées, conformément à l'article 32 (1) ii, et de réduire significativement le risque de survenance de cette violation de données.

34. La formation restreinte rappelle que l'exposition de données à caractère personnel sans contrôle d'accès préalable est identifiée comme faisant partie des vulnérabilités les plus répandues et qu'elle a déjà prononcé de nombreuses sanctions pécuniaires publiques pour des faits similaires.

35.Au regard de ces éléments, la formation restreinte considère que la société n'a pas mis en œuvre les mesures techniques et organisationnelles appropriées afin de garantir la sécurité des données personnelles traitées, conformément à l'article 32 du Règlement.

b. Sur la portée du manquement

36.La société souligne que l'exploitation de la vulnérabilité nécessitait des compétences particulières, comme le prouve l'utilisation d'un script par la délégation de contrôle, et qu'elle n'était possible qu'en ayant connaissance de l'adresse URL https://www.crm.sergic.com/documents/upload/eresa/X.pdf . La société relève par ailleurs que l'ensemble des documents contenus au sein du répertoire n'auraient pas pu être téléchargés par la délégation de contrôle. Elle fait également valoir qu'aucun utilisateur du site ne lui a rapporté que ses données personnelles avaient fait l'objet d'une utilisation malveillante.

37.La société souligne ensuite que chacun des documents fournis par les candidats à la location est nécessaire pour la constitution du dossier, notamment pour évaluer leur solvabilité, et qu'elle ne demande aux candidats aucune autre pièce que celles visées par le décret n° 2015-1437 du 5 novembre 2015 fixant la liste des pièces justificatives pouvant être demandées au candidat à la location et à sa caution.

38.Elle rappelle en outre qu'elle n'a pas la maîtrise des pièces spontanément téléchargées par les candidats alors qu'elles ne figurent pas dans le décret précité. De la même façon, la société estime qu'elle ne peut être tenue pour responsable du fait que certains candidats téléchargent leur carte Vitale en tant que justificatif d'identité ou que le numéro d'inscription au répertoire (NIR) figure sur des documents émis par des organismes sociaux que transmettent les personnes.

39.Enfin, la société explique qu'à la suite de la violation de données, elle a planifié la correction de la vulnérabilité sur plusieurs mois, ce qui a abouti à la mise en production le 17 septembre 2018 d'un correctif permettant de mettre définitivement un terme à la vulnérabilité.

La société précise que ces délais s'expliquent par la forte demande de locations en période estivale et par la difficulté de suspendre ses activités durant cette période.

40. En premier lieu, la formation restreinte observe que l'exploitation de la vulnérabilité ne requérait pas de maîtrise technique particulière en matière informatique. En effet, la simple modification de la valeur de X dans l'adresse URL https://www.crm.sergic.com/documents/upload/eresa/X.pdf permettait à toute personne ayant connaissance de l'URL précitée de télécharger les documents en question, sans que la création préalable d'un compte sur le site soit nécessaire, et sans que cela requière une manipulation plus compliquée que la simple modification de la valeur X , qui correspond à un nombre. Par ailleurs, la formation restreinte considère que l'utilisation d'un script ne nécessite aucunement de posséder des compétences avancées pour exploiter cette vulnérabilité. L'utilisation d'un script par la délégation de contrôle avait pour unique objectif d'automatiser un processus manuel consistant à modifier la valeur de X à la fin de l'adresse URL en question, pour télécharger les documents les uns après les autres de manière plus rapide.

41. En deuxième lieu, s'agissant du nombre de fichiers concernés par le défaut de sécurité, la formation restreinte observe que c'est la délégation de la CNIL qui a, de sa propre initiative, interrompu l'exécution du script afin de ne pas surcharger le serveur hébergeant le site web. Il ressort ensuite des informations transmises par la société à la délégation au cours du contrôle du 13 septembre 2018, et des constatations effectuées, que l'intégralité des documents contenus dans le répertoire en question, soit 290 870 fichiers, ont été rendus accessibles par ce défaut de sécurité. Les fichiers qui d'après la société n'auraient pu être téléchargés correspondaient à des numérotations auxquelles n'étaient pas rattachés de dossiers comme la société en a convenu à l'audience. La formation relève que, dans ses observations, la société a en outre indiqué que le nombre de personnes concernées était de 29 440.

42. En troisième lieu, la formation restreinte estime que le manquement à l'obligation de sécurité est aggravé au regard de la nature des données à caractère personnel rendues accessibles. En effet, comme exposé précédemment, les documents transmis par les candidats à la location sont de nature très diverse et figuraient notamment, parmi les documents en question, des actes de mariage, des jugements de divorce, des contrats de travail, des documents relatifs à des prestations sociales ou encore des avis d'imposition. Ces documents contiennent à la fois des données d'identification, telles que le nom, le prénom et les coordonnées, mais également une grande quantité d'informations susceptibles de révéler certains aspects parmi les plus intimes de la vie des personnes, comme les jugements de divorce.

43.La formation restreinte ne remet pas en cause la nécessité pour la société SERGIC de disposer de la plupart de ces documents. Elle rappelle néanmoins que l'article 32 du Règlement impose au responsable de traitement de mettre en œuvre des mesures de sécurité adaptées aux risques induits par le traitement pour les droits et libertés des personnes, risques résultant notamment de l'accès non autorisé aux données personnelles traitées. En outre, dans la mesure où la société SERGIC traite des documents contenant des informations très précises sur certains aspects de la vie privée des personnes, la nécessité de mettre en place des mesures

de sécurité proportionnées, permettant de garantir leur confidentialité, était d'autant plus importante. La formation restreinte rappelle sur ce point que le considérant 83 du Règlement prévoit que […] Ces mesures devraient assurer un niveau de sécurité approprié, y compris la confidentialité, compte tenu de l'état des connaissances et des coûts de mise en œuvre par rapport aux risques et à la nature des données à caractère personnel à protéger.

44. En dernier lieu, la formation restreinte note que l'existence de la vulnérabilité sur le site www.sergic.com a été portée à la connaissance de la société dès le 8 mars 2018 et n'a été résolue qu'en septembre 2018. Les données personnelles des utilisateurs ont donc été accessibles durant au moins six mois alors même que la société SERGIC en avait connaissance. Si la formation restreinte admet que la correction de la vulnérabilité pouvait nécessiter des phases d'analyse et de développements techniques, elle estime que des mesures d'urgence n'ayant pas pour objectif de corriger la vulnérabilité mais de réduire l'ampleur de la violation de données étaient techniquement simples à mettre en place et auraient pu être rapidement déployées. Par exemple, les fichiers contenus dans le répertoire rendu accessible par la vulnérabilité auraient pu être déplacés vers un répertoire temporaire ou bien une meure de filtrage des URL aurait pu être mise en œuvre pour empêcher l'accès aux documents. De surcroît, il apparaît que la société, consciente de l'augmentation de ses activités à partir du mois de mai, en raison de la forte demande de locations, a fait le choix de privilégier la stabilité de son système d'information durant cette période à la correction de la vulnérabilité des données personnelles qu'il comportait. Par conséquent, dans la mesure où le défaut de sécurité a été porté à sa connaissance dès le 8 mars 2018, et où la société savait qu'un pic d'activités interviendrait à partir du mois de mai, il lui revenait d'anticiper cette difficulté et de prendre a minima toutes les mesures nécessaires dès la connaissance de cette vulnérabilité.

5. Sur le manquement à l'obligation de conserver les données pour une durée proportionnée

45.L'article 5-1-e) du Règlement dispose que :

1. Les données à caractère personnel doivent être :

[…] e) 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) .

46.Le rapporteur reproche à la société SERGIC de conserver les documents transmis par les candidats n'ayant pas accédé à la location au-delà de la durée nécessaire à l'atteinte de la

finalité pour laquelle les données personnelles ont été collectées et traitées – à savoir la location d'un bien immobilier - et ce sans que cette conservation ne soit encadrée par des garanties appropriées.

47.En défense, la société rappelle tout d'abord que ces personnes sont susceptibles de saisir le Défenseur des droits en alléguant d'une discrimination et, qu'à ce titre, le Défenseur des droits peut exiger de la société la transmission de l'ensemble du dossier déposé par le candidat. La société précise que le délai de prescription applicable à des faits de discrimination étant de six ans, les documents sont conservés pour cette durée. Elle ajoute que la délégation de contrôle n'a pas constaté la présence dans le répertoire affecté par la vulnérabilité de document antérieur à 2012. La société souligne dans ses écritures qu'aucune pièce du dossier ne prouve l'absence d'archivage intermédiaire des données et d'une gestion des habilitations d'accès aux documents.

48.La formation restreinte rappelle que la durée de conservation des données personnelles doit être déterminée en fonction de la finalité poursuivie par le traitement. Lorsque cette finalité est atteinte, les données doivent soit être supprimées, soit faire l'objet d'un archivage intermédiaire lorsque leur conservation est nécessaire pour le respect d'obligations légales ou à des fins précontentieuses ou contentieuses. Ces données doivent alors être placées en archivage intermédiaire, pour une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont conservées, conformément aux dispositions en vigueur. Ainsi, après avoir opéré un tri des données pertinentes à archiver, le responsable de traitement doit prévoir, à cet effet, une base de données d'archives dédiée ou une séparation logique dans la base de données active. Cette séparation logique est assurée par la mise en place de mesures techniques et organisationnelles garantissant que seules les personnes ayant un intérêt à traiter les données en raison de leurs fonctions, comme par exemple les personnes du service juridique, puissent y accéder. Au-delà de ces durées de conservation des données versées en archives intermédiaires, les données personnelles doivent être supprimées.

49. En l'espèce , la formation restreinte rappelle que la collecte par la société SERGIC des données personnelles des candidats a pour finalité l'attribution de logements. Dès lors que cette finalité est atteinte, les données personnelles des candidats n'ayant pas accédé à la location ne peuvent plus être conservées au-delà de trois mois, au sein de la base de données active et au-delà faire l'objet d'une séparation logique voire d'un archivage intermédiaire.

50.Or, la formation restreinte observe que la société a indiqué à la délégation de la CNIL lors de la mission de contrôle du 13 septembre 2018 que les documents transmis par les candidats n'ayant pas accédé à la location, c'est-à-dire ceux pour lesquels la poursuite du traitement n'était plus justifiée, n'étaient pas supprimés et qu'aucune purge n'était mise en œuvre en base de données. Elle note encore que, dans ses observations en défense, la société a produit un document dont il ressort que sa politique en matière de conservation des données des clients et prospects n'a été formalisée qu'en novembre 2018. Enfin, au cours de la séance du 11 avril 2019, la société a indiqué que la mise en place d'une solution d'archivage des documents en question était en cours de réalisation.

51.Il ressort de ces différents éléments que la société SERGIC conservait en base active les données à caractère personnel des candidats n'ayant pas accédé à la location pour une durée excédant dans des proportions importantes celle nécessaire à la réalisation de la finalité du traitement, à savoir l'attribution de logements, sans qu'aucune solution d'archivage intermédiaire n'ait été mise en place.

52.Au regard de l'ensemble de ces éléments, la formation restreinte considère qu'un manquement à l'obligation de conservation des données, telle que prévue par l'article 5 du Règlement, est caractérisé.

III.Sur la sanction et la publicité

53. L'article 45-III 7° de la loi du 6 janvier 1978 dispose : Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité 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 Parlement européen et du Conseil du 27 avril 2016 précité, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83. L'article 83 du RGPD prévoit que Chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives. Selon les caractéristiques propres à chaque cas, les amendes administratives sont imposées en complément ou à la place des mesures visées à l'article 58, paragraphe 2, points a) à h), et j). Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative, il est dûment tenu compte, dans chaque cas d'espèce, des éléments suivants : a) la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi; b) le fait que la violation a été commise délibérément ou par négligence ; c) toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées; d) le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32; e) toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant; f) le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs; g) les catégories de données à caractère personnel concernées par la violation; h) la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure,

le responsable du traitement ou le sous-traitant a notifié la violation; i) lorsque des mesures visées à l'article 58, paragraphe 2, ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures; j) l'application de codes de conduite approuvés en application de l'article 40 ou de mécanismes de certification approuvés en application de l'article 42; et k) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation.

54.La société considère qu'une amende administrative de 900 000 euros est disproportionnée compte tenu des critères fixés par l'article 83 du Règlement, de ses capacités financières et des sanctions précédemment prononcées par la formation restreinte. Elle rappelle ensuite que ni le RGPD, ni la loi Informatique et Libertés ne prévoient de règles s'agissant du montant maximum de l'amende pouvant être infligée par l'autorité de contrôle lorsque les manquements retenus sont punis pour l'un, d'une amende pouvant s'élever jusqu'à 10 millions d'euros ou 2% du chiffres d'affaires annuel mondial et, pour l'autre, d'une amende pouvant s'élever jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial.

55. Tout d'abord, la formation restreinte estime que dans le cas d'espèce, les manquements précités justifient que soit prononcée une amende administrative à l'encontre de la société pour les motifs suivants.

56.D'une part, elle rappelle que face aux risques représentés par les violations de données à caractère personnel, le législateur européen a entendu renforcer les obligations des responsables de traitement en matière de sécurité des traitements. Ainsi, selon le considérant 83 du RGPD, Afin de garantir la sécurité et de prévenir tout traitement effectué en violation du présent Règlement, il importe que le responsable du traitement ou le sous-traitant évalue les risques inhérents au traitement et mette en œuvre des mesures pour les atténuer, telles que le chiffrement. Ces mesures devraient assurer un niveau de sécurité approprié, y compris la confidentialité, compte tenu de l'état des connaissances et des coûts de mise en œuvre par rapport aux risques et à la nature des données à caractère personnel à protéger. Dans le cadre de l'évaluation des risques pour la sécurité des données, il convient de prendre en compte les risques que présente le traitement de données à caractère personnel, tels que la destruction, la perte ou l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite, qui sont susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral . Or, la formation restreinte observe que le défaut de sécurité qui a rendu possible la violation de données trouve son origine dans une conception défectueuse de son site par la société SERGIC. La mise en œuvre d'une procédure d'authentification sur le site était une mesure élémentaire à prendre, qui aurait permis d'éviter la violation de données personnelles.

57.D'autre part, La formation restreinte relève que la société SERGIC a manqué de diligence dans la correction de la vulnérabilité alors qu'en présence d'une violation de données, le RGPD impose une réaction rapide. Il est ainsi prévu au considérant 85 qu' Une violation de

données à caractère personnel risque, si l'on n'intervient pas à temps et de manière appropriée, de causer aux personnes physiques concernées des dommages physiques, matériels ou un préjudice moral […] . Quand bien même aucune personne physique n'a, à ce jour, rapporté avoir subi un dommage en raison de la violation de données, le manque de célérité de la société dans la correction de la vulnérabilité, pendant une durée d'au moins six mois, a eu pour effet de prolonger le risque qu'un tel dommage ne survienne.

58. Ensuite, la gravité des violations est également à apprécier au regard des catégories de données concernées. A cet égard, la formation restreinte rappelle que les données traitées par la société dans le cadre de la gestion des dossiers des candidats locataires contiennent des informations particulièrement précises sur certains aspects de leur vie privée. Dès lors qu'elle reçoit ce type de données, la société doit apporter une attention toute particulière à la préservation de leur confidentialité et à leurs modalités de conservation ; or elle n'a pas prévu de base intermédiaire et a conservé durant une durée manifestement excessive ces données.

59.La formation restreinte rappelle par ailleurs que le § 3 de l'article 83 du Règlement prévoit qu'en cas de violations multiples, le montant total de l'amende ne peut excéder le montant fixé pour la violation la plus grave. En l'espèce, dans la mesure où il est reproché à la société un manquement à l'article 5 du Règlement, lequel peut faire l'objet d'une amende pouvant s'élever jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial, c'est ce montant maximum qu'il convient de prendre en considération.

60.Compte tenu de l'ensemble de ces éléments, la formation restreinte, tenant compte des critères fixés à l'article 83 du RGPD et de la situation financière de la société, estime qu'une amende administrative à hauteur de 400 000 euros est justifiée et proportionnée, ainsi qu'une sanction complémentaire de publicité pour les mêmes motifs.

PAR CES MOTIFS

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

de rejeter la demande de nullité soulevée par la société SERGIC ;

de rejeter la demande de la société SERGIC de ne pas prendre en considération les éléments issus de la procédure suivie contre la société SERGIC ENTREPRISES ;

de prononcer à l'encontre de la société SERGIC , une amende administrative d'un montant de 400 000 (quatre cent mille) euros ;

de rendre publique, sur le site de la CNIL et sur le site de Légifrance, sa délibération qui sera anonymisée à l'expiration d'un délai de deux ans à compter de sa publication.

Le Président / Alexandre LINDEN