Le : 25/07/2019

Date de publication sur legifrance: 25/07/2019

Commission Nationale de l'Informatique et des Libertés

Délibération n°SAN-2019-007 du 18 juillet 2019
Délibération de la formation restreinte n° SAN – 2019-007 du 18 juillet 2019 prononçant une sanction pécuniaire à l'encontre de la société ACTIVE ASSURANCES

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 Anne DEBET, Mme Sylvie LEMMET, 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 20 et suivants ;
Vu le décret n° 2019-536 du 29 mai 2019 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° 2018-136C du 26 juin 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 de tout traitement accessible à partir du domaine activeassurances.fr ou portant sur des données à caractère personnel collectées à partir de ce dernier ;
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 8 mars 2019 ;
Vu le rapport de M. François PELLEGRINI, commissaire rapporteur, du 4 avril 2019 ;
Vu les observations écrites versées par la société ACTIVE ASSURANCES le 6 mai 2019 ;
Vu les observations en réponse du commissaire rapporteur du 16 mai 2019 ;
Vu le courrier de la société ACTIVE ASSURANCES du 11 juin 2019 ;
Vu 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 13 juin 2019 :
M. François PELLEGRINI, commissaire, entendu en son rapport ;
En qualité de représentants de la société ACTIVE ASSURANCES :
M. X
Maître Y, avocate ;
Maître Z, avocate ;
Mme XX ;
La formation restreinte a entendu, en application de l'article 42 du décret n° 2019-536 du 29 mai 2019, M. XY, directeur technique au sein de la société […].
La société ayant eu la parole en dernier ;
Après en avoir délibéré, a adopté la décision suivante :

I-Faits et procédure

1. La société ACTIVE ASSURANCES (ci-après la société) est une société par actions simplifiée ayant une activité d'intermédiaire en assurance, concepteur et distributeur de contrats d'assurance automobile à des particuliers, en vente directe ou en vente en ligne. La société emploie environ 160 salariés, dont 150 sont situés à Madagascar au sein d'une succursale de la société.
2. La société a réalisé en 2018 un chiffre d'affaires de [...] euros et un résultat net de [...]euros. Son siège social est situé 71, rue de Billancourt à Boulogne-Billancourt (92100).
3. Pour les besoins de son activité, la société édite le site web www.activeassurances.fr, sur lequel les personnes peuvent demander des devis ou souscrire des contrats d'assurance automobile. La

société obtient des clients majoritairement via son site web et par le biais de comparateurs d'assurances automobiles disponibles sur d'autres sites web.
4. Le 1er juin 2018, la Commission nationale de l'informatique et des libertés (ci-après la CNIL ou la Commission) a été informée, par un client de la société ACTIVE ASSURANCES, qu'il avait accès aux données d'autres clients sans procédure d'authentification préalable. Le 27 juin suivant, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a également avisé la CNIL que l'accès aux données à caractère personnel des utilisateurs du site web de la société était possible sans contrôle préalable depuis le moteur de recherche Duckduckgo (https://duckduckgo.com).
5. En application de la décision n° 2018-136C de la présidente de la Commission du 26 juin 2018, une mission de contrôle en ligne a été réalisée par une délégation le 28 juin 2018.
6. Cette mission a eu pour objet de vérifier la conformité aux dispositions de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après loi du 6 janvier 1978 modifiée ou loi Informatique et Libertés) et au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après RGPD ou Règlement), de tout traitement accessible à partir du domaine activeassurances.fr ou portant sur des données à caractère personnel collectées à partir de ce dernier.
7. Au cours de cette mission de contrôle, la délégation a constaté qu'une requête effectuée au sein du moteur de recherche Duckduckgo à partir des mots clés client.activeassurances.fr site:client.activeassurances.fr faisait apparaître des liens hypertextes permettant d'accéder librement à certains comptes de clients de la société, sans authentification préalable. En cliquant sur ces liens, la délégation a pu accéder à des comptes de clients - comportant notamment leur nom, prénom, adresse postale, adresse électronique, numéro de téléphone - et télécharger plusieurs documents PDF concernant des personnes, tels que des pièces d'identité, des devis, des attestations d'assurance automobile ou encore des contrats d'assurance. La délégation a également constaté que la modification du numéro identifiant apparaissant à la fin d'une des adresses URL affichées dans les résultats de recherche du moteur de recherche Duckduckgo permettait d'accéder aux comptes personnels d'autres clients de la société.
8.La société a été informée par téléphone le même jour, par la délégation, de l'existence d'un défaut de sécurité sur son site. Un courrier électronique contenant le type d'adresses URL concernées lui a également été adressé. Il était demandé à la société de prendre les mesures correctives nécessaires pour y remédier dans les plus brefs délais afin d'éviter tout accès aux données personnelles par des tiers non autorisés.
9. Par courrier du 2 juillet 2018, la société a indiqué à la Commission, par l'intermédiaire de son conseil, que plusieurs mesures avaient été prises afin de remédier au défaut de sécurité. Elle précisait que l'ensemble des liens indexés au sein des différents moteurs de recherche avaient été sécurisés. De plus, elle indiquait que l'adresse URL permettant de visualiser les documents stockés au sein de l'espace de stockage Microsoft Azure, était à présent chiffrée et avait une durée de vie limitée d'une heure. La société indiquait avoir ainsi pris les mesures nécessaires pour rendre les documents inaccessibles à un utilisateur qui aurait souhaité copier le lien et l'indexer dans un moteur de recherche ou sur une application.
10. Le 12 juillet suivant, lors de la mission de contrôle dans les locaux de la société, cette dernière a informé la délégation qu'elle avait pris des mesures dès le 29 juin afin que les documents de ses clients ne soient plus accessibles à des tiers non autorisés. Elle a ainsi précisé avoir modifié le code source du site web ne générant pas d'authentification des personnes pour accéder à leur espace client, ainsi que le paramétrage des documents stockés sur le service Microsoft Azure, celui-ci étant, avant l'alerte de la CNIL, configuré de telle sorte que les fichiers étaient accessibles publiquement depuis l'Internet. La délégation a, en outre, effectué une requête à partir des mots clés client.activeassurances.fr site:client.activeassurances.fr au sein des moteurs de recherche Bing, Qwant et Yahoo. Elle a constaté qu'une liste de liens hypertextes renvoyant vers les comptes clients était toujours affichée dans les résultats de recherche mais que ceux-ci renvoyaient vers la page de connexion à l'espace client ou vers un message d'erreur ResourceNotFound . Cependant, il a été constaté qu'en cliquant sur le bouton en cache affiché à côté de l'adresse URL référencée dans les résultats de recherche, il était encore possible d'accéder à des pages contenant des données personnelles des clients.
11. La délégation a également constaté que les mots de passe de connexion des clients à leur espace personnel, dont le format est imposé par la société, correspondaient à leur date de

naissance et que ce format était indiqué sur les formulaires de connexion. Il a également été constaté que, après la création de leur compte, l'identifiant et le mot de passe de connexion étaient transmis aux clients par courriel et indiqués en clair dans le corps du message.
12.Aux fins d'instruction de ces éléments, la présidente de la CNIL a désigné, le 8 mars 2019, M. François PELLEGRINI en qualité de rapporteur sur le fondement de l'article 47 de la loi du 6 janvier 1978 modifiée, dans sa rédaction applicable à la date des faits. Par courrier du même jour, la présidente de la CNIL a informé la société de cette désignation.
13.À l'issue de son instruction, le rapporteur a fait notifier par porteur à la société ACTIVE ASSURANCES, le 5 avril 2019, un rapport détaillant le manquement relatif à l'article 32 du RGPD qu'il estimait constitué en l'espèce.
14.Ce rapport proposait à la formation restreinte de la CNIL de prononcer à l'encontre de la société ACTIVE ASSURANCES une amende administrative d'un montant de 375 000 euros et qui serait rendue publique.
15.Était également jointe au rapport une convocation à la séance de la formation restreinte du 13 juin 2019. La société disposait d'un délai d'un mois pour communiquer ses observations écrites.
16.Le 6 mai 2019, la société a produit des observations écrites sur le rapport. À cette occasion, la société a formulé une demande pour que la séance se tienne à huis-clos. Le président de la formation restreinte a rejeté cette demande par lettre du 10 mai 2019.
17.Les observations de la société ont fait l'objet d'une réponse du rapporteur le 16 mai 2019.
18.Le 11 juin 2019, la société a produit des observations. Celles-ci ayant été adressées postérieurement à l'expiration du délai de quinze jours prévu au troisième alinéa de l'article 40 du décret du 29 mai 2019, elles seront déclarées irrecevables.
19.La société et le rapporteur ont présenté des observations orales lors de la séance de la formation restreinte du 13 juin 2019.

II.Motifs de la décision

A- Sur l'absence de mise en demeure préalable

20. La société soutient que la présidente de la Commission aurait pu lui adresser une mise en demeure qui lui aurait permis d'entreprendre une démarche de mise en conformité plus approfondie à la suite du contrôle en ligne de la Commission.
21.La formation restreinte relève qu'il résulte de la lettre même des dispositions du III de l'article 20 de la loi du 6 janvier 1978 modifiée que le prononcé d'une sanction n'est pas subordonné à une mise en demeure préalable. La décision de désigner un rapporteur et de saisir la formation restreinte est un pouvoir appartenant au président de la Commission, 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.

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

1- Sur le défaut de sécurité ayant entraîné la violation de données à caractère personnel

a.Sur la caractérisation du manquement

22.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 :*
i. la pseudonymisation et le chiffrement des données à caractère personnel ;
ii. des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
iii. 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 ;
iv. une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.
23.L'article 32 (2) du Règlement 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.

24. Il appartient à la formation restreinte de déterminer si la société ACTIVE ASSURANCES a manqué à son obligation d'assurer la sécurité des données à caractère personnel traitées et si, en particulier, elle 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.

25. En défense, la société ne conteste pas qu'un défaut de sécurité ait affecté le site web www.activeassurances.fr mais souligne que, après avoir été informée de l'existence de celui-ci par les services de la Commission, elle a mis en place rapidement des mesures efficaces pour y remédier.

26. En premier lieu, tout en soulignant la diligence de la société qui a réagi rapidement après la révélation de l'incident pour le corriger, la formation restreinte relève que les mesures élémentaires de sécurité n'avaient pas été prises en amont du développement de son site web, ce qui a rendu possible la survenance de la violation de données à caractère personnel.

27. La formation restreinte relève que, lors du contrôle du 28 juin 2018, la délégation de la CNIL a pu accéder aux données de clients de la société en effectuant une recherche à partir des mots clés client.activeassurances.fr site:client.activeassurances.fr au sein du moteur de recherche Duckduckgo. Les liens hypertextes apparaissant dans les résultats des moteurs de recherche permettaient en effet d'accéder directement aux comptes des clients contenant leurs informations personnelles et des pièces justificatives, sans contrôle préalable. En outre, la délégation a constaté que les données étaient également accessibles en modifiant l'adresse URL affichée dans la barre de navigation, une telle opération pouvant être effectuée par un client de la société connecté à son espace personnel – qui pouvait ainsi accéder à d'autres comptes personnels que le sien - ou par toute personne qui voyait apparaître dans les résultats du moteur de recherche Duckduckgo les adresses URL renvoyant vers les comptes des clients de la société. Par ailleurs, lors du contrôle sur place du 12 juillet suivant, la délégation a constaté que les données et pièces justificatives des clients étaient également accessibles à partir du cache des moteurs de recherche Bing, Qwant et Yahoo.

28.La formation restreinte rappelle que lorsqu'une requête visant à accéder à une ressource est adressée à un serveur, celui-ci doit préalablement vérifier que son émetteur est autorisé à accéder aux informations demandées. Or, en l'espèce, tant le plaignant qui avait signalé ce défaut de sécurité aux services de la Commission que la délégation de contrôle, ont pu librement consulter les documents des clients enregistrés par la société, sans qu'aucune mesure de restriction n'y fasse obstacle.

29. La formation restreinte estime que la violation de données à caractère personnel résultant de ce défaut de sécurité aurait pu être évitée si, par exemple, la société avait mis en œuvre une mesure d'authentification et une gestion des droits d'accès permettant de s'assurer que chaque utilisateur souhaitant accéder à un document était habilité à le consulter.

30. Elle considère que ce défaut de sécurité démontre que, dès sa conception en 2014, le site web de la société était défectueux et que celle-ci n'avait pas mis en place les mesures appropriées et élémentaires de sécurité.

31. De plus, la formation restreinte considère que le défaut de sécurité a été amplifié par le fait que les documents des personnes, librement accessibles depuis le site web de la société, ont été indexés par les moteurs de recherche Duckduckgo, Bing, Qwant et Yahoo. Cette indexation a été rendue possible dès lors que la société n'avait pas mis en place de mesures permettant de limiter celle-ci par les moteurs de recherche, au moyen, par exemple, d'un fichier robot.txt .

32. Par ailleurs, la formation restreinte estime que la société aurait dû mettre en place ces mesures élémentaires qui ne nécessitaient pas de développements techniques importants. Elle rappelle, en outre, que les responsables de traitement sont régulièrement alertés, notamment par ses délibérations prononçant des amendes administratives, sur l'importance de mettre en place ce type de mesure afin de protéger les données des personnes.

33. En second lieu, la société soutient que l'identification du défaut de sécurité de son site web nécessitait des compétences techniques informatiques particulières, ce dont disposait le plaignant qui a effectué le signalement à la CNIL, du fait de sa profession. Elle considère qu'une personne physique non instruite dans le domaine du développement informatique n'aurait pu identifier ce défaut de sécurité et que les constatations du plaignant sont l'œuvre d'un spécialiste et qu'elles ne

sont pas représentatives de l'activité sur Internet d'une personne physique non initiée.
34. La formation restreinte considère cependant que l'accès aux données des clients de la société était possible à partir d'une manipulation simple consistant en une modification du numéro apparaissant dans l'adresse URL affichée dans le navigateur. Une telle modification ne nécessite aucune opération complexe ni aucune maîtrise technique particulière en matière informatique. Cette simple modification du numéro apparaissant dans l'adresse URL est à la portée de tout utilisateur d'un navigateur dès lors que cette adresse apparaît dans le navigateur de tout client de la société se connectant à son compte. La même manipulation pouvait également être effectuée par toute personne qui, à partir d'une recherche effectuée au sein des moteurs de recherche Duckduckgo, Bing, Qwant et Yahoo, voyait affichées dans son navigateur les adresses URL renvoyant vers les comptes des clients de la société.
35. La formation restreinte rappelle, en outre, qu'elle est régulièrement confrontée à une telle problématique et qu'elle a indiqué, dans plusieurs délibérations, qu'une telle manipulation ne nécessite aucune compétence technique particulière. Elle relève également que l'exposition de ressources sans contrôle d'accès préalable fait partie des dix failles de sécurité les plus à surveiller selon le guide 2017 des bonnes pratiques de l'Open Web Application Security Project, l'association professionnelle de référence en termes de sécurité des sociétés du web. La vérification des paramètres URL fait en outre partie de tous les audits de sécurité web, dans la mesure où il s'agit d'une attaque connue depuis longtemps par la profession des développeurs web.
36.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
37. La société explique qu'elle n'a eu connaissance du défaut de sécurité que le 28 juin 2018, à la suite de l'information des services de la Commission, et qu'elle a pris les mesures correctrices qui s'imposaient immédiatement après cette alerte. Elle précise avoir procédé rapidement au déréférencement de l'ensemble des liens indexés par le moteur de recherche Duckduckgo.com, ce dont la délégation a pris acte par courriel du 4 juillet suivant.
38. La société indique avoir également fait appel à la société […] afin de réaliser un audit complet de son système informatique et mettre ses opérations de traitements en conformité avec la règlementation. Elle précise avoir, par la suite, informé régulièrement les services de la Commission de l'état d'avancement de sa mise en conformité.
39. Elle précise enfin, dans son mémoire en défense, avoir mis en place avec la société […] un plan de remédiation, daté d'avril 2019, définissant les actions à mener. Le directeur technique de cette société a en outre précisé, lors de la séance du 13 juin, que les mesures de sécurité concernant les données à caractère personnel avaient toutes été prises.
40. En premier lieu, la formation restreinte constate que la société a mis en place les mesures correctives nécessaires à la sécurisation des données à caractère personnel et prend acte du fait qu'un plan de remédiation plus général, permettant d'assurer sa conformité avec la règlementation, a été déterminé.
41. Cependant, la formation restreinte relève que la résolution du défaut de sécurité n'a pu être effectuée qu'à la faveur d'un signalement d'un client de la société qui a tenté en vain de l'en informer en mai 2018. En outre, les mesures élémentaires nécessaires à la sécurisation des données de ses clients n'ont été mises en place par la société qu'après le signalement puis l'intervention des services de la Commission auprès de celle-ci.
42. La formation restreinte considère dès lors que la société n'a placé la sécurité des données de ses clients au cœur de ses préoccupations qu'après l'intervention des services de la Commission.
43. En second lieu, en ce qui concerne le nombre de personnes concernées par le défaut de sécurité, la formation restreinte relève que la délégation a constaté, lors du contrôle sur place, que la base contenait 148 359 numéros de téléphone distincts et 144 057 adresses électroniques distinctes concernant des clients. La société a précisé, à cette occasion, que les données personnelles et pièces justificatives relatives à tous les contrats conclus par la société, résiliés ou non, étaient librement accessibles en raison du défaut de sécurité constaté.
44. La formation restreinte relève en outre que chaque client de la société doit fournir plusieurs documents le concernant dans le cadre de la conclusion d'un contrat. Par conséquent, un grand nombre de documents étaient rendus accessibles du fait du défaut de sécurité affectant le site web

de la société, à savoir notamment 144 890 copies de carte grise, 137 776 copies de permis de conduire, 119 940 relevés d'identité bancaire, 119 517 devis ou encore 36 068 copies de déclarations de cession d'un véhicule.
45. De plus, chaque document contient, de par sa nature, de multiples informations sur la personne concernée telles que ses nom, prénom, adresse postale, adresse électronique, date et lieu de naissance, coordonnées bancaires, immatriculation du véhicule ou encore des éléments relatifs à la suspension du permis de conduire et les motifs de résiliation de garantie de la part de la société.
46. Par conséquent, le défaut de sécurité a concerné un nombre particulièrement important de données à caractère personnel et de documents concernant les clients de la société.
47. De plus, la formation restreinte relève que le défaut de sécurité a concerné des documents contenant des éléments permettant de révéler des informations particulièrement précises sur les personnes. Il était ainsi possible d'avoir accès à l'historique des clients en matière d'assurance automobile et de savoir ainsi si une personne avait fait l'objet d'une résiliation ou d'une annulation de contrat pour fausse déclaration ou pour non-paiement d'une prime, ou encore si elle avait fait l'objet d'un retrait de permis ou commis un délit de fuite ou un refus d'obtempérer.
48. Sur ce dernier point, la formation restreinte relève que les données en question sont relatives à des infractions commises par les personnes et aux suites qui leur ont été données. Elle rappelle que le considérant 83 du RGPD prévoit que les mesures permettant d'atténuer les risques inhérents au traitement doivent 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* . Par conséquent, de telles données, considérées comment étant des données particulières, doivent faire l'objet de la part des responsables de traitement d'une vigilance et d'une protection renforcées, ce qui n'a pas été le cas en l'espèce.
2- Sur l'absence de robustesse des mots de passe d'accès aux comptes clients de la société
49. La délégation de la CNIL a constaté, lors du contrôle du 12 juillet 2018, que les clients devaient se connecter à leur espace personnel accessible en ligne via leur numéro client et leur date de naissance, cette seconde information valant mot de passe. La société a informé la délégation qu'aucune mesure complémentaire pour l'authentification des personnes, telle qu'une limitation du nombre de tentatives en cas de mots de passe erronés, n'avait été mise en place.
50. Le rapporteur soutient que l'insuffisante robustesse des mots de passe ne permet pas d'assurer la sécurité des données traitées par la société et d'empêcher des attaques par force brute qui consistent à tester successivement et de façon systématique de nombreux mots de passe et conduisent, ainsi, à une compromission des comptes associés et des données personnelles qu'ils contiennent.
51. En défense, la société ne conteste pas les faits constatés, mais soutient que son choix quant à la complexité des mots de passe était guidé par le souci de faciliter les diligences de ses clients afin qu'ils puissent aisément accéder à leur dossier personnel et communiquer dans des conditions conviviales et pratiques avec leur courtier. La société avait ainsi indiqué, lors du contrôle sur place, qu'elle avait souhaité faciliter les démarches des assurés, certains ayant des difficultés à lire et à écrire. Par la suite, la société a informé la CNIL avoir imposé à ses clients, le 26 juillet 2018, une modification de leur mot de passe lors d'une nouvelle connexion à leur espace.
52. La formation restreinte relève qu'il appartient à la société ACTIVE ASSURANCES de mettre en œuvre des mesures de sécurité destinées à assurer la sécurité de toutes les données à caractère personnel qu'elle traite, y compris notamment celles des populations vulnérables. Elle relève à cet égard que des préconisations sont mises en avant par la Commission et l'ANSSI afin d'aider toute personne à créer un mot de passe complexe et facile à retenir. La formation restreinte considère donc que la société dispose de moyens lui permettant de remplir ses obligations en termes de sécurité, alors même que certains de ses clients auraient des difficultés à lire et à écrire.
53. La formation restreinte rappelle que, pour assurer un niveau de sécurité suffisant et satisfaire aux exigences de robustesse des mots de passe, lorsqu'une authentification repose uniquement sur un identifiant et un mot de passe, le mot de passe doit comporter au minimum douze caractères - contenant au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial - ou le mot de passe doit comporter au moins huit caractères - contenant trois de ces quatre catégories de caractères - et être accompagné d'une mesure complémentaire comme

par exemple la temporisation d'accès au compte après plusieurs échecs (suspension temporaire de l'accès dont la durée augmente à mesure des tentatives), la mise en place d'un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (ex : captcha) et/ou le blocage du compte après plusieurs tentatives d'authentification infructueuses.
54. La formation restreinte relève que la nécessité d'un mot de passe fort est également soulignée par l'ANSSI, qui indique qu' *un bon mot de passe est avant tout un mot de passe fort, c'est à dire difficile à retrouver même à l'aide d'outils automatisés. La force d'un mot de passe dépend de sa longueur et du nombre de possibilités existantes pour chaque caractère le composant. En effet, un mot de passe constitué de minuscules, de majuscules, de caractères spéciaux et de chiffres est techniquement plus difficile à découvrir qu'un mot de passe constitué uniquement de minuscules* .
55. En outre, il ressort des constats effectués par la délégation de contrôle que le formulaire de connexion des clients à leur espace personnel indiquait expressément le format des mots de passe de connexion, à savoir la date de naissance des personnes, ce qui facilitait considérablement une attaque par force brute, ce d'autant que le format des mots de passe était indiqué sur le formulaire de connexion au compte client. La formation restreinte relève également que les clients désirant renforcer la sécurité de leurs données et modifier leur mot de passe en étaient empêchés par la société qui avait imposé le format relatif à la date de naissance.
56. La formation restreinte considère, par conséquent, que les mots de passe mis en place par la société pour accéder aux comptes clients ne correspondaient pas aux exigences requises en termes de robustesse.
57. Enfin, en ce qui concerne la transmission des mots de passe aux clients de la société par courriel, en clair, après la création du compte, la formation restreinte relève qu'une telle procédure ne permet pas d'assurer la sécurité des données, dès lors que l'envoi d'un courriel non chiffré peut conduire à son interception par toute personne écoutant le réseau et à la prise de connaissance des informations qu'il contient.
58. La formation restreinte relève que la société n'a pas contesté, dans sa réponse ou lors de la séance, l'existence d'un tel manquement.
59. La formation restreinte en déduit que la société a méconnu une mesure de sécurité élémentaire préconisée par la CNIL alors que la transmission des mots de passe en clair dans un courriel le rend accessible à tout tiers susceptible d'accéder à la messagerie électronique de la personne concernée.
60. Sur la base de l'ensemble de ces éléments, la formation restreinte considère que le manquement à l'article 32 du Règlement est constitué.

III.Sur la sanction et la publicité

61. L'article 20-III de la loi du 6 janvier 1978 modifiée 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* .
62. L'article 83 du RGPD prévoit : *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 .

63.La société considère que le montant proposé dans le rapport de sanction est disproportionné dès lors que celui-ci équivaut à 3,5 % de son chiffre d'affaires, ainsi qu'au vu de sa réactivité et des mesures mises en place après la découverte du défaut de sécurité.

64. La société estime que de tels éléments doivent être pris en compte par la formation restreinte dans le cadre de la détermination du montant de l'amende administrative, comme cela a été fait dans le cadre de procédures antérieures. Lors de la séance du 13 juin, la société a insisté sur le fait que sa taille et sa capacité financière doivent être pris en compte dans la détermination du montant de la sanction et que le montant proposé par le rapporteur est disproportionné au vu de sanctions prononcées antérieurement à l'encontre de sociétés ayant une capacité financière plus élevée et davantage de salariés.

65. Elle souligne également sa coopération avec les services de la Commission dans le cadre des échanges entretenus avec ceux-ci à la suite des contrôles en ligne ainsi que lors du contrôle sur place et fait valoir qu'aucun de ses clients ne l'a informée de l'existence d'un dommage, à la suite de la notification de la violation de données à caractère personnel auprès de ceux-ci.

66.Tout d'abord, la formation restreinte considère 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.

67.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 la société n'a pas mesuré, avant d'être alertée par les services de la CNIL, l'importance de la sécurisation des données personnelles contenues dans ses systèmes d'information, malgré la nature des données traitées.

68. Ensuite, la formation restreinte considère que la gravité du manquement est caractérisée en l'espèce.

69. Celle-ci est caractérisée en raison de la nature des données personnelles concernées, la société traitant des données particulièrement identifiantes, ainsi que des données relatives à des infractions. La formation restreinte considère également que la gravité du manquement est

caractérisée en raison du nombre de documents et de personnes concernées par le défaut de sécurité, celui-ci ayant affecté les comptes de plusieurs milliers de clients et de personnes ayant résilié leur contrat avec la société.
70. La formation restreinte rappelle, par ailleurs, que le défaut de sécurité est dû à une conception défectueuse de son site web par la société, développé en 2014, et qu'il a donc perduré pendant plusieurs années. En outre, la mise en œuvre d'une procédure d'authentification sur le site ainsi que celle d'une directive limitant l'indexation par les moteurs de recherche de certaines parties du site web étaient des mesures élémentaires.
71. Enfin, la formation restreinte relève que les décisions de sanction invoquées par la société ont été adoptées sous l'empire de la loi Informatique et Libertés telle que modifiée par la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, qui prévoyait que le montant de sanctions pouvant être prononcées par la formation restreinte ne pouvait excéder 3 millions d'euros. Les faits de l'espèce ont eux été constatés alors que le RGPD était entré en application et que le manquement constaté est susceptible de donner lieu à une amende pouvant s'élever jusqu'à 10 000 000 d'euros ou, dans le cas d'une entreprise, jusqu'à 2% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.
72. La formation restreinte note, toutefois, que la société a réagi rapidement après avoir eu connaissance de la violation de données en mettant en place des mesures correctrices vingt-quatre heures après avoir été alertée par les services de la CNIL. Elle prend également acte de ce que la société a coopéré avec la CNIL dans le cadre des différents échanges entretenus avec ses services à la suite des contrôles et de sa bonne foi dans la résolution du défaut de sécurité.
73. Elle relève enfin que la société a informé ses clients de la survenance du défaut de sécurité et qu'aucun dommage les concernant n'a été porté à sa connaissance.
74.Compte tenu de l'ensemble de ces éléments, la formation restreinte, tenant compte des critères fixés à l'article 83 du RGPD, estime qu'une amende administrative à hauteur de 180 000 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 déclarer irrecevables les observations de la société ACTIVE ASSURANCES produites le 11 juin 2019 ;
- de prononcer à l'encontre de la société ACTIVE ASSURANCES, une amende administrative d'un montant de 180 000 (cent quatre-vingt mille) euros ;
- de rendre publique, sur le site de la CNIL et sur le site de Légifrance, sa délibération, qui n'identifiera plus nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.
Le Président
Alexandre LINDEN
Cette décision peut faire l'objet d'un recours devant le Conseil d'Etat dans un délai de deux mois à compter de sa notification.

Nature de la délibération: SANCTION