CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

SOCIÉTÉ ALAN
MONSIEUR LE PRÉSIDENT
117 QUAI DE VALMY
75010 PARIS

Paris, le 15 MARS 2021

[redacted]

A rappeler dans toute correspondance

Monsieur le Président,

Conformément à la décision n° 2020-274C, la Commission Nationale de l'Informatique et des Libertés (CNIL) a effectué, le 25 novembre 2020, un contrôle en ligne du site web « www.alan.com » et de l'application mobile « Alan : l'assurance santé qui fait du bien » mis en œuvre par la société ALAN. Ce contrôle s'est poursuivi par un contrôle sur audition le 15 décembre 2020 dans les locaux de la CNIL.

Ce contrôle avait pour objet d'apprécier la conformité des traitements mis en œuvre par la société ALAN à l'ensemble des dispositions de la loi n° 78-17 du 6 janvier 1978 modifiée ainsi qu'au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD). Les vérifications ont en particulier porté sur les traitements de données à caractère personnel mis en œuvre dans le cadre de la conclusion et l'exécution de vos contrats d'assurance complémentaire.

Les constatations effectuées, ainsi que les compléments apportés par courriel le 25 décembre 2020, le 15 janvier et le 18 février 2021, me conduisent à vous faire part des observations suivantes.

En premier lieu, la délégation a constaté que votre société a défini une politique de durées de conservation des données qui n'est pas appliquée. Il a également été précisé qu'aucune procédure d'archivage des données n'est mise en place mais que des travaux sont en cours à ce sujet et devraient aboutir à l'implémentation effective des durées définies avant la fin du premier semestre 2021, incluant la purge effective de toutes les données ayant dépassé leur durée de conservation et la mise en place d'une procédure automatique d'archivage et de purge.

S'agissant des données des prospects, je prends bonne note du fait qu'une procédure de suppression annuelle des données de prospects dont le dernier contact remonte à plus de deux années a désormais été mise en œuvre et qu'il a été procédé à la purge afférente.

Néanmoins, la périodicité annuelle de ces purges conduit à maintenir dans vos bases de données de prospects ayant dépassé, dans l'hypothèse maximale, de 364 jours la durée de conservation fixée. Dès lors, afin de vous conformer à l'article 5-1-e) du RGPD, je vous prie de mettre en place une procédure de suppression au minimum mensuelle.

Par ailleurs, la délégation a été informée lors de l'audition que, pour les personnes ayant créé

un compte mais n'ayant pas été jusqu'à l'étape de souscription du contrat, leurs données relatives à l'assurance, dont le numéro de sécurité sociale, sont conservées pour une durée de deux mois, à l'issue de laquelle seules les données permettant de réaliser de la prospection commerciale sont conservées pour une durée de deux ans. Or, j'observe que les compléments adressés à la suite de l'audition ne précisent pas si la procédure de purge précitée a également été appliquée à ces données. Dès lors, compte tenu de la sensibilité des données traitées, je vous remercie de bien vouloir vous assurer de l'effectivité de la procédure de purge ainsi que du respect de la durée de conservation définie.

Enfin, à la lecture des compléments adressés le 18 février, je relève qu'une procédure d'archivage intermédiaire est désormais définie s'agissant des données traitées dans le cadre d'une offre de complémentaire santé. Toutefois, je note que les données administratives de l'assuré et ses justificatifs de soins sont conservés en base active dix années après la fin de son contrat dans le cadre du fonctionnement de l'offre de prévoyance. Vous indiquez que la finalité de cette durée de conservation s'inscrit dans le cadre du délai de prescription applicable en matière d'assurance visé à l'article L114-1 du code des assurances.

L'article 5-1-e) du RGPD dispose que « *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* ». La délibération n° 2005-213 de la CNIL du 11 octobre 2005 portant adoption de la recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel précise notamment les règles d'archivage intermédiaire appliquées aux données conservées pour répondre à une obligation légale ou à des fins probatoires et dont les durées de conservation sont fixées par les règles de prescription applicables.

Dès lors, si les données relatives aux contrats de prévoyance peuvent être conservées au-delà de la relation contractuelle aux fins de répondre à une obligation légale ou à des fins probatoires, leur accès doit néanmoins être limité aux seules personnes ayant à en connaître en raison de leurs fonctions. Pour ce faire, vous devez conserver ces données, à l'issue de la relation commerciale, dans une base d'archive intermédiaire, avec des accès restreints.

En deuxième lieu, la délégation a constaté que le courriel reçu par le salarié l'invitant à créer un compte Alan ainsi que le formulaire d'adhésion comportent tous deux un lien renvoyant vers la Politique de confidentialité. Ce lien ne figure toutefois pas sur le formulaire de dispense permettant au salarié de refuser d'adhérer à la mutuelle. La délégation a également constaté que les documents contractuels vous liant à vos clients et adhérents ne comportent pas l'ensemble des mentions d'information prévues à l'article 13 du RGPD.

Or, je vous rappelle qu'en application des dispositions des articles 12 et 13 du règlement précité, « *Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples (...)* ». L'article 13 dresse, par ailleurs, la liste de l'ensemble des mentions devant être portées à la connaissance de l'utilisateur.

Dès lors, je vous prie de bien vouloir insérer un lien vers votre Politique de confidentialité sur l'ensemble des formulaires de collecte de données et notamment le formulaire de dispense afin de délivrer une information complète, conforme aux exigences des articles 12, 13 et 14 du RGPD. Je vous recommande également de renvoyer à ce document dans vos conditions contractuelles, y compris dans les documents contractuels vous liant à vos adhérents travailleurs non-salariés.

En troisième lieu, la délégation a constaté que les contrats que vous lui avez transmis ne

précisent pas nécessairement la qualification de sous-traitants, responsables conjoints ou simples destinataires des données des partenaires avec lesquels vous échangez des données à caractère personnel ou ne comprennent pas, lorsque la relation de sous-traitance est établie, l'intégralité des stipulations imposées par l'article 28 du RGPD.

Dès lors, je vous invite à clarifier l'encadrement juridique vous liant à vos partenaires et à compléter les contrats vous liant à vos sous-traitants afin de vous conformer aux exigences de l'article 28 du RGPD.

En quatrième lieu, je relève que le registre des incidents de sécurité et violations de données de votre société fait notamment mention, les 10 septembre 2019 et 10 juillet 2020, d'incidents de sécurité n'ayant pas fait l'objet d'une notification de violation de données à la CNIL.

Je vous rappelle qu'il vous appartient, en votre qualité de responsable de traitements, lors de la survenance d'événements de sécurité, outre de veiller à la clôture de l'incident, de mener une analyse afin de déterminer si la faille a fait l'objet d'une exploitation ayant entraîné une violation de données à caractère personnel. Si tel est le cas, vous devez alors notifier celle-ci à la CNIL en application de l'article 33 du RGPD. Par ailleurs, dans le cas où la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, l'article 34 du RGPD impose d'informer ces dernières.

Vous trouverez des informations complémentaires sur l'obligation de notification ainsi que le formulaire permettant de procéder aux démarches en ligne à partir de l'adresse suivante : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles.

Il apparaît également que, depuis la date de l'audition, vous avez procédé à la notification de quatre violations de données à la Commission. Ces notifications concernent pour la plupart des incidents à l'envergure très restreinte, et ont trait pour la plupart soit à votre processus de recrutement, soit aux échanges que vous avez avec les organismes clients de votre société ou les personnes que vous assurez. Je vous invite sur ces sujets à affermir vos procédures pour éviter la réitération de ce type d'incidents, aussi isolés soient-ils.

Ne doutant pas que vous prendrez les mesures qui s'imposent sur l'ensemble de ces points pour assurer votre mise en conformité, **je vous informe de ma décision de clore la procédure de contrôle n° 2020-274C**.

Une telle clôture ne préjuge toutefois en aucune manière de vérifications ultérieures qui pourraient être effectuées auprès de votre organisme par notre Commission.

Mes services [redacted] se tiennent à votre disposition pour toute information complémentaire.

Je vous prie d'agréer, Monsieur le Président, l'expression de mes salutations distinguées.

[redacted]

Copie adressée par courriel [redacted] à Mme Marion BERGERET, DPO