

CNIL : Sanction de 1,75 million d'euros à l'encontre d'AG2R LA MONDIALE

La CNIL a infligé une amende de 1,75 million d'euros à AG2R LA MONDIALE pour avoir manqué aux obligations du règlement général sur la protection des données (RGPD) relatives aux durées de conservation et à l'information des personnes.

Deux manquements sont principalement mis en avant : une durée excessive de conservation des données personnelles et un manque d'information lors du démarchage téléphonique par des sous-traitants.

A l'origine, la CNIL a effectué un contrôle le 29 octobre 2019 sur place au sein des locaux du groupe AG2R LA MONDIALE dans le but de vérifier la conformité des traitements mis en œuvre dans le cadre de sa mission de gestion des retraites complémentaires de salariés du secteur privé ainsi que de son activité assurantielle.

Le contrôle visait plus particulièrement les traitements de données à caractère personnel des clients et des prospects du groupe. Les vérifications opérées portaient notamment sur les durées de conservation des données à caractère personnel et sur l'information portée à la connaissance des personnes concernées s'agissant des traitements effectués par la SGAM AG2R LA MONDIALE chargée de coordonner l'activité assurantielle de prévoyance, dépendance, santé, épargne et retraite supplémentaire.

Sur la base des éléments recueillis, la CNIL a considéré que la société avait manqué à deux obligations fondamentales prévues par le RGPD, celle de limiter la durée de conservation des données et celle d'informer les personnes. Elle a ainsi prononcé une amende de 1 750 000 euros et a décidé de rendre publique sa décision.

Durée excessive de conservation des données (article 5-1-e du RGPD)

La CNIL a pu constater que si la société disposait au jour du contrôle d'un référentiel relatif aux durées de conservation des données de ses clients et prospects, celui-ci n'était toutefois pas mis en œuvre au sein de ses systèmes d'information.

S'agissant des prospects

Lors du contrôle, la CNIL a constaté la présence, en base active, des données à caractère personnel de 1917 prospects n'ayant pas eu de contact avec la société depuis plus de trois ans, dont 1405 prospects n'ayant pas eu de contact avec la société depuis plus de cinq ans, sans que la société soit en mesure de justifier de la nécessité d'appliquer des durées de conservation supérieures à la durée maximale de trois ans qu'elle avait elle-même fixée.

Pour la CNIL, la durée de trois ans constitue une durée de conservation proportionnée et conforme aux recommandations faites dans le cadre de la norme simplifiée n° NS-056 (délibération n° 2013-213 du 11 juillet 2013) concernant les traitements automatisés de données relatifs à la gestion commerciale de clients et de prospects mis en œuvre par les organismes d'assurance, capitalisation, réassurance, assistance et par les intermédiaires d'assurance.

La CNIL précise à ce sujet que si depuis l'entrée en application du RGPD le 25 mai 2018, les normes simplifiées n'ont plus de valeur juridique, elles constituent toujours un point de repère pour les responsables de traitement, leur permettant de s'assurer de leur conformité.

S'agissant des clients

Si les durées de conservation des données des clients en matière assurantielle doivent permettre de respecter les délais légaux prévus, notamment, par le code des assurances et le code de commerce, la CNIL a néanmoins constaté en pratique la conservation en base active des données à caractère personnel d'un grand nombre de clients, après le terme du contrat d'assurance, pour des durées supérieures à celles fixées par les dispositions légales applicables.

Ces données conservées étaient relatives, notamment, à l'identité, aux coordonnées personnelles, professionnelles et bancaires, à la vie personnelle et professionnelle, à l'assurance, ainsi que, dans le cadre de certains contrats, à la santé des personnes :

- les données de milliers de clients titulaires de **contrats de type incendies, accidents et risques divers**, lesquelles peuvent être conservées entre **deux ans après la fin du contrat** (article L. 114-1 du code des assurances, fixant les délais de prescription des actions dérivant d'un contrat d'assurance, aucune autre finalité n'ayant été mise en avant par la société pour justifier d'une conservation à l'issue de l'expiration des contrats) et **dix ans pour certaines pièces comptables** (article L. 123-22 du code de commerce), l'ont été pour des durées excédant dix ans et parfois supérieures à trente ans.
- les données à caractère personnel de près de cent mille clients titulaires **de contrats épargne, épargne patrimoniale, retraite supplémentaire, obsèques et prévoyance**, lesquelles peuvent être conservées pour des durées variables pouvant aller **jusqu'à trente ans après le dénouement du contrat pour la finalité de gestion des contentieux** (article L. 114-1, dernier alinéa, du code des assurances), l'ont été pour une durée supérieure. En outre, aucune autre finalité n'avait été mise en avant pour les traitements postérieurs au contrat.

- les données à caractère personnel de plus de deux millions de clients, collectées dans le cadre des **contrats santé**, ont été conservées pour des durées excédant la durée légale de **cinq ans suivant la résiliation du contrat** (délai calqué sur celui de l'article 2224 du code civil, repris dans le référentiel de la société). Pour 1,3 million de clients titulaires d'un contrat santé, la durée de conservation excédait dix ans et, pour des milliers de clients, trente ans.

D'un point de vue organisationnel, la CNIL a relevé l'absence de mécanisme d'archivage permettant la conservation des données des clients à des fins comptables, fiscales ou contentieuses dans la limite des délais de prescription que ce soit en les transférant au sein d'une base d'archives dédiée ou en mettant en place des restrictions d'accès à ces données pour qu'elles ne puissent être consultées que par des personnes spécialement habilitées, ayant un intérêt à en connaître en raison de leurs fonctions (par exemple, le service en charge du contentieux).

Information insuffisante dans le cadre du démarchage téléphonique (articles 13 et 14 du RGPD)

Les articles 13 et 14 (l'article 14 concerne le cas où les données à caractère personnel ne sont pas collectées directement auprès de la personne concernée) du RGPD imposent au responsable de traitement de fournir à la personne concernée différentes informations relatives notamment à son identité et ses coordonnées, aux finalités du traitement mis en œuvre, sa base juridique, les destinataires ou les catégories de destinataires des données, au fait que le responsable du traitement a l'intention d'effectuer un transfert de données vers un pays tiers, etc.

Lors du contrôle, la CNIL a constaté que la SGAM AG2R LA MONDIALE confiait à ses sous-traitants une partie des opérations de prospection téléphonique à mener auprès de ses clients et prospects. Des scripts d'appels étaient établis par la société ou ses filiales. 30% des conversations téléphoniques sortantes effectuées par ses deux sous-traitants étaient enregistrées à des fins d'amélioration de la qualité du service de la SGAM AG2R LA MONDIALE.

L'écoute d'un échantillon des cinquante derniers appels téléphoniques passés par ces deux sous-traitants a permis à la CNIL de constater :

- l'absence d'information des personnes contactées, soit du principe même de l'enregistrement de l'appel, soit de leur droit à s'y opposer ;
- l'absence d'information, même sommaire, relative au traitement de leurs données à caractère personnel ou aux autres droits dont elles disposent à l'égard de leurs données ;
- l'absence de possibilité d'obtenir une information plus complète relative à la protection de leurs données à caractère personnel, par exemple via l'envoi d'un courriel ou l'activation d'une touche sur leur clavier téléphonique.

SOULIER BUNCH

Soulier Bunch est un cabinet d'avocats pluridisciplinaire proposant aux différents acteurs du monde industriel, économique et financier une offre de services juridiques complète et intégrée.

Nous assistons nos clients français et étrangers sur l'ensemble des questions juridiques et fiscales susceptibles de se poser à eux tant dans le cadre de leurs activités quotidiennes qu'à l'occasion d'opérations exceptionnelles et de décisions stratégiques.

Chacun de nos clients bénéficie d'un service personnalisé adapté à ses besoins, quels que soient sa taille, sa nationalité et son secteur d'activité.

Pour plus d'informations, visitez soulierbunch.com.

Le présent document est fourni exclusivement à titre informatif et ne saurait constituer ou être interprété comme un acte de conseil juridique. Le destinataire est seul responsable de l'utilisation qui pourrait être faite des informations qu'il contient.