



Délibération SAN-2021-010 du 20 juillet 2021

Commission Nationale de l'Informatique et des Libertés Nature de la délibération : Sanction

Etat juridique : En vigueur

Date de publication sur Légifrance : Jeudi 22 juillet 2021

Délibération de la formation restreinte n°SAN-2021-010 du 20 juillet 2021 concernant la société SGAM AG2R LA MONDIALE

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de Monsieur Alexandre LINDEN, président, Monsieur Philippe-Pierre CABOURDIN, vice-président, Monsieur Bertrand du MARAIS, Madame Christine MAUGÛE et Monsieur Alain DRU, membres ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 20 et suivants ;

Vu le décret no 2019-536 du 29 mai 2019 pris pour l'application de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération no 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2019-164C du 26 septembre 2019 de la présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification des traitements mis en œuvre par le groupe AG2R LA MONDIALE ou pour son compte ;

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 12 novembre 2020 ;

Vu le rapport de Madame Sophie LAMBREMONT, commissaire rapporteure, notifié à la SGAM AG2R LA MONDIALE le 26 avril 2021 ;

Vu les observations écrites versées par la SGAM AG2R LA MONDIALE le 26 mai 2021 ;

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 17 juin 2021 :

Madame Sophie LAMBREMONT, commissaire, entendue en son rapport ;

En qualité de représentants de la SGAM AG2R LA MONDIALE, s'étant exprimés lors de la séance :

[...]

La SGAM AG2R LA MONDIALE ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. La Société de groupe d'assurance mutuelle AG2R LA MONDIALE (ci-après "la SGAM AG2R LA MONDIALE" ou "la société") est une société d'assurance mutuelle créée le 16 janvier 2008. Son siège social est situé [...] à Paris [75008].

2. La SGAM AG2R LA MONDIALE appartient au groupe AG2R LA MONDIALE (ci-après "le groupe"), organisme français de protection sociale et patrimoniale remplissant, d'une part, une mission de gestion administrative des retraites complémentaires des salariés du secteur privé et, d'autre part, une activité assurantielle. Le groupe assure environ 15 millions personnes en France, à titre individuel ou à titre collectif, et accompagne plus de cinq-cent-mille entreprises. Le groupe emploie environ dix-mille collaborateurs.

3. Au sein du groupe, la SGAM AG2R LA MONDIALE est chargée de coordonner l'activité assurantielle de prévoyance, dépendance, santé, épargne et retraite supplémentaire. Elle compte plusieurs filiales, parmi lesquelles figurent notamment les sociétés [...] et [...].

4. En 2019, le chiffre d'affaires généré par l'activité assurantielle menée par la SGAM AG2R LA MONDIALE s'élevait à 9,6 milliards d'euros pour un résultat net de 350 millions d'euros. En 2020, son chiffre d'affaires s'élevait à 9,3 milliards d'euros pour un résultat net de 222 millions d'euros.

5. Le 29 octobre 2019, en application de la décision n° 2019-164C du 26 septembre 2019 de la présidente de la Commission, une délégation de la CNIL a mené une opération de contrôle sur place au sein des locaux du groupe AG2R LA MONDIALE. Cette mission avait pour objet de vérifier le respect par le groupe AG2R LA MONDIALE de l'ensemble des dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après "le Règlement" ou "le RGPD") et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après "la loi du 6 janvier 1978 modifiée" ou "la loi Informatique et Libertés").

6. Le contrôle visait plus particulièrement les traitements de données à caractère personnel des clients et des prospects du groupe. Les vérifications opérées ont notamment porté 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.

7. A l'issue du contrôle, le procès-verbal n° 2019-164/1 a été notifié à la SGAM AG2R LA MONDIALE, par courrier daté du 30 octobre 2019. Le 12 novembre 2019, la société a transmis à la CNIL les pièces complémentaires demandées lors du contrôle. A la suite de demandes complémentaires formulées par les services de la Commission, la société a fourni de nouveaux éléments et pièces les 9 décembre 2019, 17 janvier et 10 février 2020.

8. Aux fins d'instruction de ces éléments, la présidente de la Commission a, le 12 novembre 2020, désigné Madame Sophie LAMBREMON en qualité de rapporteure, sur le fondement de l'article 22 de la loi du 6 janvier 1978 modifiée.

9. À l'issue de son instruction, la rapporteure a, le 26 avril 2021, fait notifier à la SGAM AG2R LA MONDIALE un rapport détaillant les manquements au RGPD qu'elle estimait constitués en l'espèce et indiquant à la société qu'elle disposait d'un délai d'un mois pour communiquer ses observations écrites en application des dispositions de l'article 40 du décret n° 2019-536 du 29 mai 2019. Le courrier de notification du rapport précisait à la société que le dossier était inscrit à la séance de la formation restreinte du 17 juin 2021.

10. Ce rapport proposait à la formation restreinte de la Commission de prononcer une injonction de mettre en conformité les traitements avec les dispositions des articles 5-1-e), 13 et 14 du RGPD, assortie d'une astreinte par jour de retard à l'issue d'un délai de trois mois suivant la notification de la délibération de la formation restreinte, ainsi qu'une amende administrative. Il proposait également que cette décision soit rendue publique, mais qu'il ne soit plus possible d'identifier nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

11. Le 3 mai 2021, par l'intermédiaire de son conseil, la société a demandé à consulter le dossier de la procédure dans les locaux de la CNIL. Le 6 mai 2021, une consultation s'est tenue dans les locaux de la CNIL, au cours de laquelle le conseil de la société a pris copie des pièces souhaitées.

12. Le 26 mai 2021, par l'intermédiaire de son conseil, la société a produit des observations en réponse au rapport de sanction.

13. Le 11 mai 2021, la société a formulé une demande pour que la séance devant la formation restreinte se tienne à huis clos. Par courrier du 20 mai 2021, le président de la formation restreinte a rejeté cette demande.

14. La société et la rapporteure ont présenté des observations orales lors de la séance de la formation restreinte du 17 juin 2021.

II. Motifs de la décision

A. Sur le manquement à l'obligation de conserver les données à caractère personnel pour une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées en application de l'article 5-1-e) du RGPD

15. Aux termes de l'article 5-1 e) du Règlement, les données à caractère personnel doivent être "conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation)".

1. Sur la conservation des données à caractère personnel des prospects

16. La rapporteure a tout d'abord relevé que, lors du contrôle le 29 octobre 2019, la société avait indiqué à la délégation que les sociétés du groupe AG2R LA MONDIALE disposaient d'un référentiel fixant les durées de conservation des données à caractère personnel des prospects (issus de fichiers tiers loués) et des clients (personnes titulaires d'un contrat individuel assurantiel auprès de la société ou de ses filiales). Néanmoins, la société a déclaré lors de ce même contrôle que les durées de conservation définies dans ce référentiel n'étaient effectivement pas mises en œuvre au sein de ses systèmes d'information, à l'exception des traitements relatifs à la lutte contre le blanchiment, aux actions locales et aux données de santé. Elle a précisé qu'un plan de mise en œuvre de la politique de confidentialité était prévu et aurait dû débiter au cours du premier semestre 2020.

17. La rapporteure a ensuite relevé que le référentiel relatif aux durées de conservation et le registre des traitements du groupe prévoyaient, pour la prospection visant le réseau de vente à distance, la conservation des données à caractère personnel des prospects pour une durée maximale de trois ans après l'enregistrement en base de données ou le dernier contact à l'initiative du prospect. Or, par courrier en date du 12 novembre 2019, la société a fourni à la délégation de contrôle une extraction provenant de l'application dédiée à la prospection commerciale pour la vente à distance,

montrant la présence des données de prospects n'ayant pas eu de contact avec la société depuis plus de trois ans, parfois depuis plus de cinq ans.

18. Dans ses observations du 27 mai 2021, la société a tout d'abord souligné qu'un référentiel relatif aux durées de conservation des données à caractère personnel des clients et prospects ayant bien été défini, aucun manquement ne pouvait lui être reproché au titre de la définition des durées de conservation.

19. Ensuite, la société a expliqué avoir entrepris des actions afin de respecter la durée de conservation maximale des données à caractère personnel des prospects telle que définie à la fois dans son référentiel et dans le registre des traitements du groupe.

20. La formation restreinte relève que, s'agissant de la définition des durées de conservation applicables aux données des prospects de la société, il y a tout d'abord lieu de relever qu'au jour du contrôle, un référentiel relatif aux durées de conservation des données des clients et prospects avait bien été établi pour les sociétés du groupe AG2R LA MONDIALE, mais que les durées de conservation y étant définies n'étaient, selon les déclarations faites par la société lors du contrôle, "pas effectivement implémentées dans le système d'information de la société, hormis s'agissant des traitements relatifs à la lutte contre le blanchiment, aux actions locales ainsi qu'aux données de santé".

21. La formation restreinte relève ensuite que, lors du contrôle du 29 octobre 2019, la délégation 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. La formation restreinte relève que la durée de trois ans constitue une durée de conservation proportionnée et conforme aux recommandations faites par la CNIL 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. 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.

22. La formation restreinte note par ailleurs que la société atteste, depuis le contrôle, avoir formulé et exécuté des requêtes en suppression des données des prospects et mettre en œuvre des purges mensuelles des données des prospects dans la base de données sous-jacente à l'application dédiée à la prospection commerciale pour la vente à distance.

23. Dès lors, si la formation restreinte prend note de ce que la SGAM AG2R LA MONDIALE met désormais en œuvre les durées de conservation définies dans le référentiel précité et le registre des traitements du groupe, permettant ainsi que les données à caractère personnel des prospects ne sont pas conservées pour des durées excédant celles nécessaires au regard des finalités pour lesquelles elles sont traitées, elle relève qu'au jour du contrôle, les durées de conservation que la société avait définies, et qui correspondent aux durées nécessaires à l'atteinte des finalités poursuivies, n'étaient pas respectées. La société a ainsi conservé les données à caractère personnel de ses prospects pendant des durées excessives, en l'absence de justification particulière, et alors que ceux-ci n'avaient montré aucun intérêt pour les produits et services proposés par la société durant plus de trois, voire de cinq ans.

2. Sur la conservation des données à caractère personnel des clients

24. Ainsi qu'il a été indiqué ci-dessus (point 16), la société disposait au jour du contrôle d'un référentiel relatif aux durées de conservation des données de ses clients et prospects, lequel n'était toutefois pas mis en œuvre au sein de ses systèmes d'information, excepté s'agissant des traitements relatifs à la lutte contre le blanchiment, aux actions locales et aux données de santé.

25. Dans le cadre de son rapport, la rapporteure a souligné qu'il devait être tenu compte de la spécificité de la matière assurantielle lors de l'appréciation du caractère proportionné de la durée de conservation des données des clients par une société d'assurance. En particulier, 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. Cependant, en l'espèce, la rapporteure a constaté que par courrier du 12 novembre 2019, la société avait fourni des documents montrant 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. Les 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.

26. En défense, la société a indiqué avoir engagé des actions correctives depuis le contrôle et a produit des justifications en vue d'attester de ses démarches de mise en conformité.

27. La formation restreinte relève tout d'abord qu'il ressort des éléments communiqués par la société postérieurement au contrôle du 29 octobre 2019, que 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.

28. Ensuite, la formation restreinte constate que 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.

29. En outre, la formation restreinte relève que 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). Elle relève également que la durée de conservation des données de 1,3 million de clients titulaires d'un contrat santé excède dix ans tandis que celle de milliers de clients excède trente ans.

30. Enfin, la formation restreinte relève qu'hormis pour les données concernant les prestations de santé, il n'existait pas, au jour du contrôle, 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).

31. La formation restreinte observe par ailleurs qu'en défense, la société n'a pas apporté d'éléments de nature à justifier de telles durées de conservation des données. A l'inverse, elle a indiqué avoir engagé un large plan de mise en conformité. A cet égard, la société a notamment expliqué qu'un projet informatique avait été initié dès 2017 afin de parvenir à une mise en œuvre effective et intégrale des durées de conservation des données relatives à ses clients. La société a précisé que le déploiement du projet informatique aurait dû s'achever en mai 2018, mais que le calendrier n'avait pu être tenu en raison de la complexité des systèmes d'information du groupe AG2R LA MONDIALE et de l'interdépendance des applications. La société a ainsi indiqué avoir défini une nouvelle stratégie de suppression des données des clients sur trois années, fondée sur une approche par les risques et le cycle de vie des données, selon le calendrier suivant :

2020 : périmètre traitements sensibles (action sociale, lutte contre le blanchiment) ;

2021 : périmètre santé-prévoyance ;

Juin 2021 : échéance du processus d'anonymisation des données liées aux produits d'épargne ;

2022 : périmètre épargne et retraite supplémentaire (cycles de vie des données plus longs - actions se prescrivant par trente ans).

32. La formation restreinte relève que la société a fourni au soutien de ses engagements des justificatifs de suppression des données de clients déjà effectuées, en 2020 et 2021, conformément au projet informatique défini, sur plusieurs applications rattachées au périmètre Santé-Prévoyance . En outre, la société a fourni un document daté du mois de mai 2021 montrant que le processus d'anonymisation des données des clients liées aux produits d'épargne était en cours.

33. Dès lors, si la formation restreinte prend note que la SGAM AG2R LA MONDIALE a fourni des éléments attestant des démarches entreprises pour garantir que les données à caractère personnel de ses clients ne sont plus conservées pour des durées excédant celles nécessaires au regard des finalités pour lesquelles elles sont traitées, elle estime qu'au jour du contrôle, ces données étaient conservées pour des durées excessives. La formation restreinte constate par ailleurs que le manquement subsiste en partie à ce jour, dans la mesure où la mise en œuvre des durées de conservation des données des clients n'est pas entièrement déployée dans les systèmes d'information de la société. En particulier, il ressort des pièces fournies par la société que la quasi-totalité du périmètre "Santé Prévoyance" serait en conformité d'ici la fin de l'année 2021 et que les travaux relatifs au périmètre "Epargne retraite" se poursuivraient en 2022. La société a précisé dans ses observations en défense et confirmé lors de la séance de la formation restreinte que les travaux de mise en conformité relatifs à la mise en œuvre des durées de conservation des clients dans ses systèmes d'information s'achèveraient à la fin de l'année 2022.

34. Au regard de l'ensemble de ces éléments, la formation restreinte considère que le manquement à l'article 5-1-e) du RGPD est caractérisé.

B. Sur le manquement relatif à l'obligation d'informer les personnes en application des articles 13 et 14 du RGPD

35. Les articles 13 et 14 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. En outre, la réglementation impose, lorsque cela apparaît nécessaire pour garantir "un traitement équitable et transparent" des données personnelles en l'espèce, d'informer les personnes sur la durée de conservation des données, l'existence des différents droits dont bénéficient les personnes, l'existence du droit de retirer son consentement à tout moment et le droit d'introduire une réclamation auprès d'une autorité de contrôle.

36. L'article 14 du RGPD, qui concerne la situation dans laquelle les données à caractère personnel ne sont pas collectées directement auprès de la personne concernée, prévoit que cette dernière doit également être informée des catégories de données à caractère personnel concernées ainsi que, si cela est nécessaire pour garantir un traitement équitable et transparent, de la source dont proviennent ces données. En outre, il précise que ces informations doivent être communiquées à la personne concernée "dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas un mois, eu égard aux circonstances particulières dans lesquelles les données à caractère personnel sont traitées ou si les données à caractère personnel doivent être utilisées aux fins de la communication avec la personne concernée, au plus tard au moment de la première communication à ladite personne" .

37. La rapporteure a relevé, ainsi qu'il ressort des constatations effectuées lors du contrôle sur place du 29 octobre 2019, que la SGAM AG2R LA MONDIALE confiait à ses sous-traitants [...] et [...] une partie des opérations de prospection téléphonique à mener auprès de ses clients et prospects. Dans ce cadre, la délégation de la CNIL a été informée que des scripts d'appels étaient établis par la société ou ses filiales et que 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.

38. La rapporteure a relevé que l'écoute d'un échantillon des cinquante derniers appels téléphoniques passés par ces deux sous-traitants a permis 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. En outre, la rapporteure a également souligné que, dans le cadre de ces enregistrements, les personnes n'étaient rendues destinataires d'aucune 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. Enfin, ces personnes ne se voyaient pas offrir la 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.

39. En défense, la société a indiqué avoir procédé à des rectifications immédiates, dès l'issue du contrôle sur place, afin de délivrer aux personnes concernées une information conforme aux exigences du RGPD. Elle a ainsi déclaré que, depuis la fin de l'année 2019, des instructions écrites relatives à l'information des personnes concernées étaient remises aux sous-traitants [...] et [...], tout comme des scripts d'appels téléphoniques actualisés contenant la plupart des mentions exigées par les articles 13 et 14 du RGPD. La société a précisé que lesdits scripts avaient été complétés avec d'ultimes mentions manquantes en 2021. Enfin, la société a indiqué qu'une notice d'information dédiée aux traitements mis en œuvre dans le cadre de l'enregistrement des appels téléphoniques sortants était désormais fournie au sein de la rubrique "protection des données" du site internet d'AG2R, indiquant la base légale du traitement et précisant les destinataires des enregistrements ainsi que les modalités d'exercice des droits. La société a précisé que les personnes démarchées téléphoniquement étaient désormais informées, par le téléopérateur, du fait qu'elles pouvaient consulter cette notice d'information en se rendant sur le site internet d'AG2R.

40. La formation restreinte relève qu'à la date du contrôle, les personnes démarchées téléphoniquement par les sociétés [...] et [...] pour le compte de la SGAM AG2R LA MONDIALE n'étaient pas correctement informées des traitements de données à caractère personnel mis en œuvre, en méconnaissance des dispositions applicables du RGPD. En effet, d'une part, les informations essentielles relatives en particulier au principe même de l'enregistrement de l'appel ou, selon les cas, au droit de s'y opposer, aux finalités de l'enregistrement et à sa durée de conservation, n'étaient pas communiquées aux personnes concernées par les sous-traitants de la SGAM AG2R LA MONDIALE. D'autre part, la formation restreinte souligne l'absence d'instructions données par la SGAM AG2R LA MONDIALE à ses sous-traitants afin de porter à la connaissance des personnes concernées les mentions d'information obligatoires prévues par le RGPD. En outre, elle relève que les scripts d'appels téléphoniques destinés au sous-traitant [...] ne contenaient aucune mention relative à la fourniture d'une quelconque information relative à la protection de leurs données à caractère personnel aux personnes concernées.

41. Au vu de ce qui précède, la formation restreinte considère qu'au jour du contrôle, la société ne respectait pas les dispositions des articles 13 et 14 du RGPD.

42. La formation restreinte relève néanmoins que, depuis le contrôle, la société s'est mise en conformité avec les exigences découlant des articles 13 et 14 du RGPD. A cet égard, la formation restreinte constate que les téléconseillers des prestataires [...] et [...] délivrent de manière effective une information aux personnes démarchées téléphoniquement concernant l'identité du responsable de traitement, le principe et la finalité de l'enregistrement de la conversation, les destinataires des enregistrements, leur durée de conservation, l'existence des droits dont disposent les personnes concernées, ainsi que la possibilité d'obtenir des informations complémentaires relatives aux traitements de données à caractère personnel mis en œuvre par la société en consultant la rubrique "protection des données" du site internet d'AG2R (au sein de laquelle est disponible la notice d'information dédiée aux traitements mis en œuvre dans le cadre de l'enregistrement des appels téléphoniques sortants).

43. Dès lors, la formation restreinte considère que les faits précités constituent un manquement aux articles 13 et 14 du RGPD, mais que la société a justifié s'être mise en conformité en fournissant, à la date de clôture de l'instruction, une information complète aux personnes démarchées téléphoniquement au sens des dispositions précitées.

III. Sur les mesures correctrices et leur publicité

44. Aux termes du III de l'article 20 de la loi du 6 janvier 1978 modifiée :

"Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut également, le cas échéant après lui avoir adressé l'avertissement prévu au I du présent article ou, le cas échéant en complément d'une mise en demeure prévue au II, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes : [...]"

2° Une injonction de mettre en conformité le traitement avec les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie, sauf dans des cas où le traitement est mis en œuvre par l'État, d'une astreinte dont le montant ne peut excéder 100 000 € par jour de retard à compter de la date fixée par la formation restreinte ; [...]"

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 total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du règlement (UE) 2016/679 du 27 avril 2016, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83."

45. L'article 83 du RGPD prévoit que "Chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives", avant de préciser les éléments devant être pris en compte pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de cette amende.

46. En premier lieu, la société fait valoir que si une amende devait être prononcée, la formation restreinte devrait tenir compte des mesures adoptées dans le sens d'une mise en conformité. S'agissant des durées de conservation des données

des prospects, la société souligne que des actions correctrices ont été rapidement déployées afin de supprimer les données des prospects dont la durée maximale de conservation est atteinte et que des purges régulières sont désormais effectuées. S'agissant des durées de conservation des données des clients, elle rappelle que la complexité des systèmes d'information du groupe AG2R LA MONDIALE a retardé la mise en œuvre pleine et entière des durées légales de conservation, celle-ci étant toutefois en cours et déjà partiellement réalisée. Lors de la séance de la formation restreinte, la société a indiqué avoir investi au total [...] depuis plusieurs années. Par ailleurs, la société souligne que l'information délivrée aux personnes démarchées téléphoniquement respecte désormais les exigences des articles 13 et 14 du RGPD. La société invite enfin la formation restreinte à tenir compte de sa pleine coopération lors de la procédure et souligne une diminution de son chiffre d'affaires et de son résultat net.

47. La formation restreinte rappelle qu'elle doit tenir compte, pour le prononcé d'une amende administrative et pour la détermination de son montant, des critères précisés à l'article 83 du RGPD, tels que la nature, la gravité et la durée de la violation, les mesures prises par le responsable du traitement pour atténuer le dommage subi par les personnes concernées, le degré de coopération avec l'autorité de contrôle et les catégories de données à caractère personnel concernées par la violation.

48. En outre, la formation restreinte rappelle que dans la mesure où sont en l'espèce reprochés à la société des manquements aux articles 5-1-e), 13 et 14 du Règlement, le montant maximum de l'amende pouvant être retenu s'élève à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

49. La formation restreinte considère tout d'abord que la société a fait preuve d'une négligence grave au regard de l'atteinte portée à des principes fondamentaux prévus par le RGPD, à savoir le principe de limitation de la durée de conservation des données et l'obligation d'informer les personnes concernées des traitements de leurs données à caractère personnel.

50. La formation restreinte relève ensuite que le manquement relatif aux durées de conservation a concerné un nombre très important de personnes, en particulier des clients de la société. En effet, la conservation en base active pour des durées supérieures aux durées légales autorisées, pouvant excéder trente ans, a concerné les données à caractère personnel de plus de deux millions de clients collectées lors de la conclusion de contrats d'assurance.

51. La formation restreinte souligne par ailleurs que, parmi les données des clients conservées pour des durées excessives, figurent des données de nature sensible, des coordonnées bancaires et des informations relatives à la vie personnelle des clients.

52. La formation restreinte relève également que les mesures de mise en conformité mises en place à la suite du contrôle n'ont pas permis de remédier entièrement au manquement relatif aux durées de conservation des données en tant qu'il concerne les clients, lequel persiste encore partiellement à ce jour. En tout état de cause, les mesures de mise en conformité adoptées n'exonèrent pas la société de sa responsabilité pour le passé.

53. De plus, la formation restreinte considère que les investissements réalisés par la société pour parvenir à la mise en œuvre des durées de conservation définies dans ses systèmes d'information ne sont pas disproportionnés au regard de son chiffre d'affaires, de la taille du groupe et de l'ampleur des travaux à réaliser compte tenu de la complexité desdits systèmes d'information soulignée par la société elle-même, qui préexistait à l'entrée en application du RGPD. La formation restreinte considère que c'est précisément le manque d'anticipation qui a contribué à des échecs dans la mise en œuvre des durées de conservation des données des clients de la société au sein de ses systèmes et, partant, à l'absence de mise en conformité avec le RGPD plus de trois ans après son entrée en application.

54. Enfin, la formation restreinte rappelle que les amendes administratives doivent être dissuasives mais proportionnées. Elle considère en particulier que l'activité de la société et sa situation financière doivent être prises en compte pour la détermination de la sanction et notamment, en cas d'amende administrative, de son montant. Elle relève à ce titre que la société fait état d'une diminution de son chiffre d'affaires, passé de 9,7 milliards en 2019 à 9,3 milliards en 2020, comme de son résultat net, passé de 350 millions en 2019 à 222 millions en 2020. Si la formation restreinte constate le résultat net a diminué de manière assez significative, elle souligne que celui-ci reste largement positif. Au vu de ces éléments, la formation restreinte considère que le prononcé d'une amende de 1 750 000 euros apparaît justifié, compte tenu notamment de la nécessité de sanctionner des manquements à des principes élémentaires du RGPD, commis par un acteur majeur de la protection sociale en France, concernant plusieurs millions de personnes et portant sur des données de nature sensible ou particulière, comme les coordonnées bancaires.

55. En conséquence, la formation restreinte considère qu'il y a lieu de prononcer une amende administrative de 1 750 000 euros au regard des manquements aux articles 5-1-e), 13 et 14 du RGPD.

56. En deuxième lieu, une injonction de mettre en conformité le traitement avec les dispositions des articles 5-1-e), 13 et 14 du RGPD a été proposée par la rapporteure dans son rapport de sanction.

57. En défense, la société soutient que les actions qu'elle a mises en œuvre s'agissant de l'ensemble des manquements relevés doivent conduire à ne pas donner suite à la proposition d'injonctions de la rapporteure.

58. S'agissant du manquement à l'obligation de définir et de respecter une durée de conservation des données à caractère personnel proportionnée à la finalité du traitement en application de l'article 5-1-e) du RGPD, la société indique avoir entrepris de nombreuses actions et avoir réalisé les investissements conséquents susmentionnés pour atteindre la mise en conformité sur ce point.

59. La formation restreinte relève, s'agissant des données des prospects, que la société met désormais en œuvre les durées de conservation définies par la société dans son référentiel, qui sont proportionnées aux finalités poursuivies et au demeurant conformes aux recommandations faites par la CNIL en la matière. S'agissant des données des clients, la société témoigne s'être engagée dans une démarche sérieuse de mise en conformité. A cet égard, la formation restreinte note d'ailleurs que la société documente avoir mené à bien une partie importante de la mise en œuvre de ces durées de conservation dans ces systèmes, seuls restant à couvrir une partie résiduelle du périmètre "Santé Prévoyance" ainsi que le

périmètre "Epargne et retraite supplémentaire", et que la société s'est engagée à achever sa mise en conformité au 31 décembre 2022.

60. S'agissant du manquement à l'obligation d'information des personnes en application des articles 13 et 14 du RGPD, la formation restreinte prend acte de la mise en conformité de la société sur ce point. En effet, la société démontre avoir envoyé des instructions écrites à ses prestataires afin que soit délivrée une information complète aux personnes démarchées téléphoniquement pour son compte, et y avoir joint des scripts d'appels complétés des mentions d'information obligatoires. Par ailleurs, l'écoute des échantillons d'appels téléphoniques communiqués par la société atteste de la délivrance effective de ces informations aux personnes concernées. En outre, une notice d'information dédiée à ces traitements et contenant des informations complémentaires a été insérée au sein de la politique de confidentialité. La personne est désormais systématiquement informée par le téléopérateur, au début de l'appel téléphonique, du fait qu'elle peut prendre connaissance de cette notice en se rendant sur le site internet d'AG2R.

61. Au vu de ce qui précède, la formation restreinte considère qu'il n'y a plus lieu de maintenir les injonctions proposées.

62. En troisième lieu, la formation restreinte considère que la publicité de la sanction se justifie au regard du fait que les manquements aux principes élémentaires du RGPD relevés en l'espèce concernent un acteur majeur de la protection sociale et patrimoniale en France, qui gère les données à caractère personnel de millions de personnes. La formation restreinte relève que dans ce contexte, la publicité de la sanction permet d'informer les personnes concernées de la nature et de l'étendue de ces manquements.

PAR CES MOTIFS

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

- prononcer à l'encontre de la SGAM AG2R LA MONDIALE une amende administrative d'un montant de 1 750 000 (un million sept-cent-cinquante-mille) euros ;

- 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 d'un an à compter de sa publication.

Le président

Alexandre LINDEN

Cette décision est susceptible de faire l'objet d'un recours devant le Conseil d'État dans un délai de deux mois à compter de sa notification.