FBConseil
AVOCAT AU BARREAU DE PARIS

Octobre 2021

Lutte contre le crime financier – Concilier les dispositions du RGPD sur le traitement des données personnelles et les contrôles de vigilance.

Les professions de la finance et de l'assurance sont soumises à des obligations réglementaires de contrôle de connaissance et suivi de leurs clients et tiers[1] dans le cadre de la lutte contre le crime financier (blanchiment de capitaux, financement du terrorisme, sanctions internationales, fraude, corruption, trafic d'êtres humains…). Ces contrôles de vigilance nécessitent le traitement de données personnelles. Comment concilier cette obligation règlementaire avec les dispositions du Règlement européen Général sur la Protection des Données personnelles (n° 2016/679, dit « RGPD ») entrées en application le 25 mai 2018 ?

- Les professions de la finance et de l'assurance dites « règlementées » et décrites aux dispositions de l'article L 561-2 du Code monétaire et financier sont tenues de procéder à une identification de leurs clients et tiers partenaires, qu'il s'agisse d'individus assurés personnes physiques, ou de dirigeants, représentant légaux ou bénéficiaires effectifs des clients personnes morales. Cette identification consiste en des contrôles de connaissance et de suivi réguliers avant l'entrée en relation et tout au long de la relation commerciale[2].

- Ces contrôles incluent :
  - la collecte d'informations et de documents justificatifs d'identité (état civil, coordonnées, nationalité) non qualifiées de données sensibles au sens de l'article 9 du RGPD.[3]
  - leur vérification,
  - une opération de filtrage dans un outil automatisé visant à comparer les données personnelles recueillies au regard de centaines de listes internationales d'individus identifiés comme exerçant des activités liées au crime financier.

- Des questions se posent quant à l'articulation entre le respect du RGPD et la mise en œuvre des dispositions légales et règlementaires sur les contrôles de vigilance.

[1] Partenaires, fournisseurs, intermédiaires de 1er rang.
[2] Art. L 561-4-1 à L 561-14-2 CMF
[3] Art.9 RGPD : "*Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.*"

➢ **Le traitement de données personnelles dans ce contexte est-il licite et compatible avec les exigences du RGPD ?**

- L'article 6 du RGPD prévoit qu'un traitement de données personnelles n'est licite que si, et dans la mesure où, au moins l'un des motifs suivants est réuni :
  - Le consentement des personnes
  - Le contrat, ou des mesures pré-contractuelles
  - Une obligation légale
  - La sauvegarde des intérêts vitaux d'une personne
  - L'intérêt public / autorité publique
  - Les intérêts légitimes du responsable de traitement

- Dans le cadre de la lutte contre le crime financier le recueil et le traitement des données personnelles des clients et des tiers par les compagnies et les intermédiaires d'assurance est bien licite en ce qu'ils se justifient par :
  - des obligations légales et règlementaires notamment prévues dans les dispositions du Code monétaire et financier transposant en droit français les Directives européennes relatives à la LCB-FT[4], ainsi que de la Loi Sapin 2 du 9 Décembre 2016 pour la lutte anti-corruption[5].
  - des mesures (pré)contractuelles dans la mesure où les données personnelles collectées auprès d'un client sont nécessaires à la souscription et à la gestion du contrat d'assurance.
  - les intérêts légitimes du responsable de traitement selon l'article 6.1 f), lequel est assorti d'un Considérant 47[6] précisant les conditions dans lesquelles un intérêt peut être considéré comme légitime *:*

    « (…) Un tel intérêt légitime pourrait, par exemple, exister lorsqu'il existe une relation pertinente et appropriée entre la personne concernée et le responsable du traitement dans des situations telles que celles où la personne concernée est un client du responsable du traitement ou est à son service. En tout état de cause, l'existence d'un intérêt légitime devrait faire l'objet d'une évaluation attentive, notamment afin de déterminer si une personne concernée peut raisonnablement s'attendre, au moment et dans le cadre de la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée. Les intérêts et droits fondamentaux de la personne concernée pourraient, en particulier, prévaloir sur l'intérêt du responsable du traitement lorsque des données à caractère personnel sont traitées dans des

[4] A ce jour six directives européennes dédiées à la LCB-FT ont été transposées en droit français, la 6ème directive européenne du 23 octobre 2018 (2018/1673) n'ayant été que partiellement transposée en droit français.

[5] La loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite "Sapin 2", publiée au Journal officiel du 10 décembre 2016

[6] Chap. II - Principes, Article 6 - Licéité du traitement - Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données – Entrée en vigueur en France le 25/05/2018

circonstances où les personnes concernées ne s'attendent raisonnablement pas à un traitement ultérieur.(…) »

Le RGPD ajoute dans le Considérant 47 une mention sur la prévention de la fraude ce qui là aussi légitime un traitement par un acteur de l'assurance :
« Le traitement de données à caractère personnel strictement nécessaire à des fins de prévention de la fraude constitue également un intérêt légitime du responsable du traitement concerné.(…)» Le RGPD n'aborde aucun des sujets connexes que sont notamment la LCB-FT et la lutte anti-corruption. En l'absence de position prise par la CNIL sur le sujet, si l'on venait à considérer que le Considérant 47 s'applique à ces domaines connexes (la fraude pouvant être un vecteur de LCB-FT ou de corruption) encore faudrait-il pour que le traitement soit licite au sens de l'article 6 du RGPD que la personne concernée « *s'attende raisonnablement* » à un traitement de ses données personnelles à une fin donnée, ce qui suppose que le responsable de traitement l'en ait préalablement informé en toute transparence.

- La collecte et le traitement des données personnelles effectuées par les professions assujetties aux dispositions du Code monétaire et financier sont donc licites et compatibles avec les dispositions du RGPD.

➢ **Quelle est la durée de conservation des données personnelles dans le cadre de la lutte contre le crime financier ?**

- Le traitement des données personnelles doit respecter les dispositions de l'article 5 du RGPD selon lequel : « *les principes généraux relatifs au traitement des données supposent qu'elles soient adéquates, pertinentes et non excessives au regard des finalités du traitement, qu'elles soient exactes et mises à jour, ou encore qu'elles ne soient pas conservées pour une durée excessive.* » Un organisme ne peut ainsi conserver des données personnelles de manière illimitée.

- Le RGPD ne définit pas la durée précise pendant laquelle les données personnelles doivent être conservées. Il appartient donc au responsable de traitement d'identifier et d'évaluer ses besoins opérationnels, notamment en se référant aux délais de prescription[7] afin d'apprécier les durées de conservation au cas par cas[8].

- Une sanction a ainsi été rendue par la CNIL en formation restreinte à l'encontre de la compagnie AG2R La Mondiale le 22 juillet 2021 à hauteur de 1.75M€ pour non-respect des dispositions de l'article 5.1 e).[9]La CNIL a considéré que la compagnie d'assurance n'avait pas mis en œuvre dans ses systèmes les durées de conservation qu'elle avait définies dans son

[7] Article 2224 Code civil (délai de prescription de droit commun) et Art L114-1 Code des assurances
[8] Voir sur ce sujet notre Fiche pratique n°6 d'octobre 2021 sur les délais de conservation des données personnelles et la gestion des contrats d'assurance
[9] https://www.cnil.fr/fr/sanction-1-75-million-deuros-ag2r-la-mondiale

référentiel et qu'elle conservait les données personnelles de ses prospects et clients sur des durées excessives.

- Dans le secteur de l'assurance, on distingue les traitements de données réalisés en dehors de la conclusion d'un contrat d'assurance de ceux mis en œuvre dans le cadre d'un contrat. Selon la CNIL[10] pour la gestion de cas de fraude, il convient de distinguer deux étapes

- L'appréciation de la pertinence de l'alerte : à partir de l'émission de l'alerte, l'organisme dispose **de six mois** pour qualifier l'alerte de pertinente ou de non pertinente. Il est recommandé de **supprimer sans délai** les alertes qualifiées de non pertinentes après analyse et traitement. Encore une fois, on peut se demander si ce court délai est applicable en cas de soupçons de CB-FT ou d'alerte de corruption[11] en l'absence de mention dans les textes règlementaires dédiés, les Lignes directrices de l'ACPR ou le Guide actualisant le Pack de conformité assurance CNIL FFA de Juillet 2021 lequel n'évoque que la gestion des risques de fraudes[12].

- La conservation de l'alerte qualifiée de pertinente : si l'alerte est « pertinente », les données ne peuvent être conservées **plus de cinq ans** à compter de la clôture du dossier de fraude.

- Ce délai de cinq ans a été retenu pour la conservation des données personnelles traitées dans le cadre général de la lutte contre le crime financier par les professionnels assujettis au Code monétaire et financier. Ainsi, les Lignes directrices de l'ACPR relatives à l'identification ou la vérification de l'identité et la connaissance de la clientèle du 27 décembre 2018 précisent que « *conformément à l'article L. 561-12, les organismes financiers conservent l'ensemble des documents et informations recueillis à l'égard de leur clientèle, y compris le bénéficiaire effectif, pendant **5 ans** à compter :*

- de l'exécution de l'opération pour les clients occasionnels ou
- de la rupture/cessation des relations d'affaires.
*Ils conservent également – sous réserve de dispositions plus contraignantes – les documents et informations portant sur les opérations réalisées par leur clientèle **pendant cinq ans** à compter de l'exécution de ces opérations ainsi que les éléments recueillis au titre de l'examen renforcé effectué en application de l'article L. 561-10-2.* ».[13]

[10] https://www.cnil.fr/fr/les-durees-de-conservation-des-donnees-du-secteur-de-lassurance
[11] En matière de lutte anti-corruption la loi Sapin 2 précise qu'en l'absence de diligences de la personne destinataire de l'alerte à vérifier, dans un délai raisonnable, la recevabilité du signalement, celui-ci est adressé à l'autorité judiciaire, à l'autorité administrative ou aux ordres professionnels. (Art.8) Aucune mention n'est faite au délai de conservation des données collectées dans le cadre d'une alerte.
[12] Guide actualisant le Pack de conformité assurance CNIL FFA de Juillet 2021
[13] https://acpr.banque-france.fr/sites/default/files/media/2018/12/17/lignes_directrices_relatives_a_lidentification_la_verification_de_lidentite_et_la_connaissance_de_la_clientele_.pdf (p. 36)

- Un délai de cinq ans à compter de l'exécution des opérations peut paraître raisonnable toutefois, dans la mesure où il se rajoute à l'obligation de conservation durant toute la relation commerciale les délais de conservation des données personnelles peuvent en réalité être beaucoup plus longs.

- Notons également qu'en pratique l'interprétation de l'ACRP sur la mise en œuvre de ce délai de cinq ans à compter de l'exécution des opérations est pour le moins extensive dans la mesure où elle considère lors de ses contrôles que le délai est applicable y compris en cas de cession de portefeuilles impliquant un transfert de propriété des données avant l'expiration dudit délai ! Il n'est pas certain que cette interprétation soit partagée par la CNIL…En tout état de cause, les professions assujetties au Code monétaire et financier doivent s'organiser pour respecter les délais impartis de conservation des données dans leurs fichiers par la règlementation comme par la « soft law ».

➢ **Un intermédiaire d'assurance ou un assureur est-il tenu de prévoir les modalités techniques et opérationnelles d'effacement à tout moment des données personnelles collectées auprès des personnes physiques dans le cadre des contrôles d'identification règlementaires** ? **Autrement dit, le « droit à l'oubli » bénéficie t'il aux souscripteurs (dirigeants et bénéficiaires effectifs inclus), aux bénéficiaires de prestations d'assurance ou aux tiers personnes physiques objets de ces contrôles** ?

- L'article 40 de la Loi informatique et Libertés du 6 janvier 1978[14] dispose que « *toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient […] effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite*. » En l'espèce les éléments d'identification des clients et des tiers collectés dans le cadre des dispositions du Code monétaire et Financier doivent être complets et régulièrement actualisés tout au long de la relation commerciale (à l'entrée en relation, au renouvellement d'un contrat d'assurance, avant tout règlement de sinistre.)

- L'article 17.1 du RGPD prévoit qu'une personne a le droit d'obtenir d'un responsable de traitement l'effacement de ses données « *dans les meilleurs délais* » notamment lorsque l'un des motifs suivants s'applique :

- Les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles sont collectées ou traitées ;
- La personne concernée a retiré son consentement au traitement de ses données et il n'existe pas d'autre fondement juridique au traitement ;
- La personne a exercé son droit d'opposition et il n'existe pas de motif légitime impérieux pour le traitement ;
- Le traitement est illicite ;
- L'effacement correspond au respect d'une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis ;

[14] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

- Les données ont été collectées dans le cadre de l'offre de services de la société de l'information pour les mineurs.

- La notion du droit à l'effacement des données personnelles ou « droit à l'oubli » prévue à l'article 17 du RGPD apparaît comme un remède aux écueils de la transparence potentiellement attentatoire à nos droits que porte le numérique. Or ce droit n'est pas absolu. En effet, l'article 17.3 b) du RGPD déroge au principe de ce « droit à l'oubli » lorsque « le *traitement est nécessaire pour respecter une obligation légale qui requiert le traitement prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement.*[15]» En l'espèce, cette dérogation s'applique puisque le traitement des données personnelles recueillies dans le cadre de la lutte contre le crime financier relève d'obligations légales et réglementaires pour les professions règlementées du marché de l'assurance.

- Toutefois, l'article 17.3 b) du RGPD ne précise pas quand cette dérogation est susceptible de s'appliquer. Faut-il comprendre que le droit à l'oubli ne peut pas s'exercer en l'espèce pendant la durée de la relation commerciale et durant le délai légal de cinq ans à compter de l'exécution des opérations, mais qu'il pourrait être exercé à l'issu de ce délai par les personnes concernées en l'absence d'initiative prise par les responsables de traitement ?

- Autrement dit, les personnes concernées par les contrôles de connaissance et suivi effectués par les professions réglementées seraient fondées à invoquer le droit à l'effacement de leurs données personnelles qui ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées au-delà du délai légal de 5 ans mais pas pendant la phase de traitement et de conservation.

- Au surplus, rappelons que conformément à l'article 14 alinéa 5, d) du RGPD l'information des personnes dont les données à caractère personnel sont indirectement collectées, et qui doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée (ex : contrôles en matière de LCB-FT), ne sont pas communiquées[16].

---

[15] Art. 7.3.b) « *Les paragraphes 1 et 2 ne s'appliquent pas dans la mesure où ce traitement est nécessaire:*
a) à l'exercice du droit à la liberté d'expression et d'information;
b) pour respecter une obligation légale qui requiert le traitement prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;
c) pour des motifs d'intérêt public dans le domaine de la santé publique, conformément à l'article 9, paragraphe 2, points h) et i), ainsi qu'à l'article 9, paragraphe 3;
d) 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, dans la mesure où le droit visé au paragraphe 1 est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement; ou
e) à la constatation, à l'exercice ou à la défense de droits en justice. »

[16] Art.14.5.d) RGPD : *« Les paragraphes 1 à 4 ne s'appliquent pas lorsque et dans la mesure où:*
d) les données à caractère personnel doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par le droit de l'Union ou le droit des États membre, y compris une obligation légale de secret professionnel. »

- Pour les acteurs de l'assurance la conformité au RGPD tout en assumant ses obligations en matière de contrôles règlementaires est une priorité majeure, d'autant que les pénalités pour non-conformité au RGPD peuvent atteindre 20 millions d'euros (ou 4 % du chiffre d'affaires global de l'entreprise).

- Les acteurs de l'assurance doivent donc plus que jamais :

- faire preuve de clarté et de transparence dans l'information des personnes physiques objets de ces contrôles quant aux conditions et modalités de traitement de leurs données personnelles en rappelant les obligations légales et règlementaires auxquelles ils sont soumis,
- s'organiser pour respecter les délais impartis par les règlementations et la « soft law » en matière de conservation et d'effacement des données personnelles dans leurs bases de données. Ceci implique d'une part, que les systèmes d'exploitation pouvant dater de plusieurs décennies soient mis en conformité pour éviter des durées de conservations illicites de dix ou trente ans déconnectées d'une finalité explicitement annoncée aux clients et, d'autre part, que soit rédigée et mise en œuvre une politique d'archivage des données entrant dans le cadre du contrôle interne, que les données soient stockées dans un cloud ou au sein d'un serveur de l'entreprise. Si une opération de traitement est confiée à un sous-traitant, le contrat de sous-traitance doit préciser les obligations de chaque partie et intégrer les exigences de l'article 28 du RGPD. Le responsable de traitement communiquera à son sous-traitant les durées et conditions de conservation à appliquer pour chaque traitement concerné.

****