CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

NS 16

La passation, la gestion et l'exécution des contrats d'assurance

Suite à l'entrée en application du RGPD, les normes adoptées par la CNIL n'ont plus de valeur juridique depuis le 25 mai 2018.

Dans l'attente de la production de référentiels RGPD, les responsables de traitement peuvent s'en inspirer pour orienter leurs premières actions de conformité.

La CNIL attire toutefois l'attention sur la nécessité de veiller au respect des nouvelles règles.

La passation, la gestion et l'exécution des contrats d'assurance

(Déclaration N° 16)

Les traitements de données personnelles au regard de la loi informatique et libertés

La mise en place d'un traitement de données personnelles doit respecter la loi I&L. En effet, toute personne qui souhaite traiter des données personnelles est soumise à un certain nombre d'obligations légales.

Finalités poursuivies par le traitement

Finalité 1 : passation et la gestion des contrats[1] :

- La passation des contrats : Il s'agit de « l'étude des besoins spécifiques de chaque demandeur afin de proposer des contrats adaptés » notamment dans le cadre du respect de l'obligation de conseil (art. L.520.1 et L.132271 du Code des assurances). Cette obligation nécessite de préciser les exigences et besoins du souscripteur éventuel, et les raisons justifiant le conseil donné pour un produit d'assurance déterminé. Cela concerne aussi « l'examen, l'acceptation, le contrôle et la surveillance du risque ». On parle couramment de « l'appréciation des risques ». Elle comprend l'examen et l'évaluation des caractéristiques du risque pour en déterminer en particulier la fréquence, son coût moyen, le coût du sinistre maximum possible, afin d'établir une tarification et de vérifier l'assurabilité du risque[2] ;
- La gestion des contrats : La gestion des contrats couvre la phase pré contractuelle jusqu'à la résiliation du contrat. Il s'agit notamment de la tarification, de l'émission des documents pré contractuels, contractuels et comptables, de l'encaissement des primes ou cotisations, de leur répartition éventuelle entre les coassureurs et les réassureurs, du commissionnement, de la surveillance des risques, et des autres opérations techniques nécessaires. Aucune décision refusant un contrat à une personne ne pourra avoir pour seul fondement un traitement automatisé de données à caractère personnel, les personnes concernées devront être mises en mesure de présenter leurs observations.

Finalité 2 : l'exécution des contrats[3] :

Il s'agit des opérations techniques nécessaires à la mise en œuvre des garanties et des prestations. Dans ce cadre, les données collectées sont relatives à la gestion des prestations, à la gestion des sinistres. Dans certains cas, il est possible que l'apériteur[4] procède à la collecte de ces informations auprès des coassureurs et des réassureurs au moment de la souscription du contrat d'assurance ou lors de l'exécution des dispositions contractuelles.

(1) Le terme contrat fait référence aux contrats d'assurance, de capitalisation, de réassurance, et d'assistance.
(2) L'assureur a l'obligation de respecter des règles prudentielles qui le conduisent à définir une politique d'acceptation des risques et refuser les risques qu'il ne peut assurer selon cette politique (article R.33612° du code des assurances et article 41 de la directive 2009/138).
(3) Le terme contrat fait référence aux contrats d'assurance, de capitalisation, de réassurance, et d'assistance.
(4) En matière d'assurance couverte par plusieurs assureurs, celui d'entre eux qui, d'une manière générale, représente le groupe d'assureurs.

Finalité 3 : l'élaboration des statistiques et études actuarielles.

Finalité 4 : l'exercice des recours et la gestion des réclamations et des contentieux.

Finalité 5 : l'exécution des dispositions légales, réglementaires et administratives en vigueur à l'exception de celles qui relèvent d'une formalité particulière prévue par la loi I&L :

Il peut s'agir de traitements relatifs à l'exécution des règles fiscales, sociales, ou encore à la collecte de contributions pour différents fonds (ex : fonds de garantie des assurances obligatoires, fonds de prévention des risques naturels majeurs). Les dispositions qui relèvent d'un régime particulier sont par exemple, celles dont les données sont soumises à un régime d'autorisation (ex : NIR, données d'infraction…) ou encore, celles relevant de la réglementation spécifique à un secteur (ex : lutte anti blanchiment…).

Catégories de données

Une fois les personnes informées de la mise en œuvre du traitement, les données qui les concernent doivent être pertinentes et proportionnées au regard de la finalité.

Les données relatives à l'identification : Il s'agit « des données relatives à l'identification des personnes parties, intéressées ou intervenantes au contrat : état civil ainsi que les pièces justifiant l'identité, les coordonnées et la nationalité ».

- **Les personnes parties et intéressées au contrat** sont notamment les assurés, les bénéficiaires, les ayants droits, les tiers, les témoins, les souscripteurs, les héritiers, les tuteurs, les curateurs, les payeurs de prime, les conducteurs, les cautions…
- **Les personnes intervenantes au contrat** sont notamment les intermédiaires en assurance, les gestionnaires, les prestataires (ex : les réparateurs automobiles, les agents de recherche privé, les experts, les avocats, les médecins, les enquêteurs, les professionnels de santé, les réseaux de soins, les officiers ministériels : notaires, huissiers…).

Les documents d'identification pouvant être collectés sont relatifs à :

- **L'état civil** : il s'agit notamment des noms, prénoms, sexe, civilité, données relatives aux pièces d'identité (permis de conduire, carte identité, livret de famille, carte de séjour, passeport…), date de décès, nom jeune fille, date et lieu de naissance…
- **Aux coordonnées** : il s'agit notamment des adresses, numéros de téléphone (fixe et mobile), numéro de télécopie et adresses électroniques, code interne de traitement permettant l'identification du client…
- **À la nationalité** : connaître la nationalité exacte des personnes parties ou intéressées au contrat permet à l'assureur de savoir : s'il peut proposer un contrat d'assurance à une personne ne résidant pas dans l'Union Européenne, ou la législation applicable au contrat d'assurance si cette personne réside dans l'UE[5]. La nationalité est l'une des informations qui permet de déterminer quelles sont les éventuelles obligations (ex : fiscales à l'égard de l'État dont le souscripteur est un ressortissant).

(5) Règlement n°593/2008 du 17 juin 2008 relatif à la loi applicable aux obligations contractuelles Rome I

ATTENTION

Conclure un contrat d'assurance avec une personne étrangère a pour conséquence le respect de la législation de son pays notamment en matière fiscale (réglementation FATCA ou convention fiscale applicable).

Les données relatives à la situation familiale, économique, patrimoniale et financière :

Il s'agit « des données relatives à la situation familiale, économique, patrimoniale et financière » des personnes parties ou intéressées au contrat et nécessaires à son application.

- **Les données relatives à la situation économique et financière sont les éléments relatifs aux** : revenus du travail et autres revenus, aux valeurs mobilières, au patrimoine immobilier, aux encours et à l'endettement, aux titres détenus, aux relevés de comptes titres, aux données d'imposition, aux crédits, aux revenus imposables, au numéro de chèque, au numéro de carte bancaire, à la date de fin de validité de la carte bancaire, aux frais généraux, au capital souscrit / remboursé, aux références bancaires (RIB, IBAN, BIC, relevé postal) à la situation de surendettement ou d'ouvrant droit à avantages assurantiels bénéficiaires CMU, RSA…
- **La situation patrimoniale** : concerne les biens du patrimoine (notamment les biens immobiliers) ;
- **La situation familiale** : concerne la situation matrimoniale (mariage, pacs, concubinage…), la composition du foyer, le nombre de personnes composant le foyer, le nombre et l'âge du ou des enfant(s)…

Les données relatives à la situation professionnelle :

Il s'agit « des données relatives à la situation professionnelle » des personnes parties ou intéressées au contrat (souscripteurs, assurés, adhérents…) et nécessaires à son application.

Sont concernés : la catégorie socioprofessionnelle, le domaine d'activité, la profession et selon les catégories de contrat : l'employeur, les catégories de personnels assurés, la branche, la convention collective, le n° SIRET / SIREN, la raison sociale, les revenus ou le chiffre d'affaires, la date prévisionnelle de départ à la retraite, le régime fiscal, les compétences et qualifications professionnelles, les justificatifs de demandeur d'emploi…

Les données nécessaires à l'appréciation du risque :

la situation géographique, les caractéristiques du logement ou du local, les conditions d'occupation, les renseignements sur les biens assurables, le type et les caractéristiques du ou des biens assurés, les informations relatives à la sinistralité et les antécédents, le permis de conduire et sa validité, et le cas échéant si le bien est utilisé sur le lieu de travail et lors de déplacements professionnels, éléments entraînant une déchéance de garantie…

Les données nécessaires à la passation, l'application du contrat et à la gestion des sinistres et des prestations :

Il s'agit des données :

- liées au contrat : le numéro d'identification du client, de l'assuré, du contrat, du dossier sinistre, le mode de paiement, les primes, les cotisations et accessoires, les commissions, les taxes, les créances en cours, les références de l'apporteur, des coassureurs et des réassureurs, la durée, les garanties, les montants, les exclusions, l'autorisation de prélèvement, les données relatives aux moyens de paiement ou relatives aux transactions telles que le numéro de la transaction, le détail de l'opération relative au produit ou service souscrit, les impayés, le recouvrement…
- liées au sinistre : la nature du sinistre, les indemnités, la valeur assurée et les garanties souscrites, la description des atteintes aux biens, les rapports d'expertise, les rapports d'enquête…
- liées à la victime : le taux invalidité/incapacité, les rentes, le capital décès, les montants des prestations, la fiscalité, les modalités de règlement, la réversion, les indemnités chômage, les montants remboursés par la sécurité sociale pour les complémentaires frais de soins (maladie, maternité…)…

Les informations relatives à la détermination ou à l'évaluation des préjudices.

Les données relatives à la localisation des personnes ou des biens :

Ces données sont des informations essentielles dans le cadre des garanties d'assistance et d'assurance (recherches des véhicules perdus ou volés, écoconduite, assistance aux personnes malades ou en difficultés…).

Les données relatives à la vie personnelle et aux habitudes de vie :

Il s'agit « des données relatives à la situation personnelle et aux habitudes de vie en relation avec les risques assurés » et nécessaires à l'application du contrat.

- **Les données relatives à la situation personnelle** sont la situation de famille, le régime juridique particulier applicable à la situation de famille, le nombre d'enfants, les descendants, les ascendants et personnes à charge, les études et la formation, la capacité et le régime de protection (minorité, tutelle, curatelle) et invalidité…
- **Les données relatives aux habitudes de vie** sont les loisirs, activités sportives et de plein air, la pratique de la chasse, de la plaisance, les trajets, les kilométrages parcourus...

Les données relatives à la santé :

Au moment de la conclusion d'un contrat il faut obtenir l'accord de l'intéressé pour le recueil de ses données de santé. C'est aussi le cas au moment de la gestion du sinistre sauf impossibilité (ex : personne en incapacité physique ou intellectuelle de consentir du fait de ses préjudices corporels).

Cette obligation n'existe pas non plus en matière de gestion des sinistres automobile, puisque l'assureur a une obligation légale de recueillir des données médicales[6] (descriptions des atteintes, copies des certificats médicaux et autres pièces justificatives, numéro de sécurité sociale) pour proposer une indemnisation aux victimes.

Dans certains cas et lorsque la sauvegarde de la vie de la personne et l'urgence des situations prévalent, il n'est pas toujours possible de recueillir le consentement de la victime au moment de sa prise en charge.

Durées de conservation

Des données lors de la conclusion d'un contrat :

Les durées de conservation doivent permettre de respecter les délais de prescriptions qui résultent, notamment, du code des assurances[7] et du code civil[8]. En outre, l'assureur a une obligation[9] de conserver les données du relevé d'information détaillant les antécédents d'une personne en tant qu'assurée auto ou moto au cours des 5 dernières années.

Des données en l'absence de conclusion d'un contrat :

Les données peuvent être conservées pendant un délai de 3 ans à compter de leur collecte par le responsable de traitement ou du dernier contact émanant du prospect (demande de renseignements ou de documentation, par exemple).

(6) Article R.21137 du code des assurances.
(7) Articles L 1141 et L 1142 du code des assurances.
(8) Les articles 2224 à 2227.
(9) Article A.1211 et 12 du code des assurances.

Des données relatives à la carte bancaire :

• Ces données doivent être supprimées lorsque la transaction est réalisée soit au moment de son paiement effectif. Dans le cas d'un paiement par carte bancaire, elles peuvent être conservées pour une finalité de preuve pendant 13 mois suivant la date de débit[10] en cas d'éventuelle contestation de la transaction. Ce délai peut être étendu à 15 mois pour tenir compte des cartes de paiement à débit différé ;
• Enfin, il est possible de conserver plus longtemps les données de la CB avec le consentement exprès du client (ex : case à cocher. En revanche cet accord ne peut pas résulter de l'acceptation de conditions générales) ;
• Les données du cryptogramme visuel ne doivent pas être stockées ;
• Lorsque la date d'expiration de la carte bancaire est atteinte, les données relatives à celles-ci doivent être supprimées.

Des données de santé :

• Si le contrat n'a pas été conclu : le responsable de traitement peut conserver les données de santé pendant une durée maximale de 5 ans[11] (2 années en archivage courant et 3 ans en archivage intermédiaire). Cette durée se justifie par le fait que le responsable de traitement doit pouvoir répondre aux demandes formulées par un assuré pour des décisions de révision de son contrat ou à des demandes de médiation.

Destinataires

Les destinataires ayant accès aux données à caractère personnel sont les personnes habilitées et agissant dans le cadre de leurs attributions.

Dans le cadre des missions habituelles :

- les personnels chargés de la passation, la gestion et l'exécution des contrats,
- les délégataires de gestion, les intermédiaires d'assurance, les partenaires ;
- les prestataires ;
- les sous-traitants, ou les entités du groupe d'assurance auquel appartient le responsable de traitement dans le cadre de l'exercice de leurs missions ;
- s'il y a lieu les organismes d'assurance des personnes impliquées ou offrant des prestations complémentaires ;
- s'il y a lieu les coassureurs et réassureurs ainsi que les organismes professionnels et les fonds de garanties ;
- les personnes intervenant au contrat tels que les avocats, experts, auxiliaires de justice et officiers ministériels, curateurs, tuteurs, enquêteurs et professionnels de santé, médecins conseils et le personnel habilité ;
- Les organismes sociaux lorsque les régimes sociaux interviennent dans le règlement des sinistres ou lorsque les organismes d'assurances offrent des garanties complémentaires à celles des régimes sociaux.

En qualité de personnes intéressées au contrat :

- Les souscripteurs, les assurés, les adhérents et les bénéficiaires des contrats et s'il y a lieu, leurs ayants droit et représentants ;
- S'il y a lieu les bénéficiaires d'une cession ou d'une subrogation des droits relatifs au contrat ;
- S'il y a lieu le responsable, les victimes et leurs mandataires ; les témoins, les tiers intéressés à l'exécution du contrat.

(11) C'est aussi le délai de prescription des actions civiles (article 2224 du code civil).
(10) Article L. 13324 du code monétaire et financier.

En qualité de personnes habilitées au titre des tiers autorisés :

- S'il y a lieu les juridictions concernées, les arbitres, les médiateurs ;
- Les ministères concernés, autorités de tutelle et de contrôle et tous organismes publics habilités à les recevoir ;
- Les services chargés du contrôle tels que les commissaires aux comptes et les auditeurs ainsi que les services chargés du contrôle interne.

Information et droits des personnes

La personne doit être informée, préalablement à la mise en œuvre du traitement :

de l'identité du responsable de traitement, de la finalité du traitement, des destinataires des données, du transfert éventuel de ses données hors UE ainsi que des droits dont elle dispose au titre de la loi I&L.

À ce titre, elle dispose d'un droit d'accès, de rectification et d'opposition.

L'information des personnes sur le site internet :

Les données de connexion (date, heure, adresse Internet, protocole de l'ordinateur du visiteur, page consultée) pourront être exploitées à des fins de mesure d'audience et d'assistance technique. Dans ce cas, le consentement préalable des personnes n'est pas nécessaire, à condition qu'ils disposent d'une information claire et complète délivrée par l'éditeur du site internet, d'un droit d'opposition, d'un droit d'accès aux données collectées et qu'elles ne soient pas recoupées avec d'autres traitements tels que les fichiers clients.

- Cette information peut, par exemple, figurer dans les courriers électroniques, sur la page d'accueil du site ou dans les conditions générales d'utilisation ;
- Le droit d'opposition à l'analyse de sa navigation : l'outil permettant de désactiver la traçabilité mise en œuvre par l'outil d'analyse de fréquentation doit remplir les conditions suivantes :
    - Un accès et une installation aisés pour tous les internautes sur l'ensemble des terminaux, des systèmes d'exploitation et des navigateurs internet ;
    - Aucune information relative aux internautes ayant décidé d'exercer leur droit d'opposition ne doit être transmise à l'éditeur de l'outil d'analyse de fréquentation.
- Tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a déjà été au préalable, de la finalité de toute action tendant à accéder à des informations déjà stockées dans son équipement terminal de communications électroniques ou à inscrire des informations dans cet équipement et des moyens dont il dispose pour s'y opposer ;
    - Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son accord ;
    - Ces dispositions ne sont pas applicables si l'accès ou l'inscription aux informations stockées a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ou est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.

Mesures de sécurité

Les mesures de sécurité « classiques » :

- Le responsable du traitement prend toutes précautions utiles pour préserver la sécurité et la confidentialité des données traitées ;
- Il définit une politique de sécurité adaptée aux risques présentés par les traitements et à la taille de l'organisme d'assurance. Cette politique devra décrire les objectifs de sécurité, et les mesures de sécurité physique, logique et organisationnelle permettant de les atteindre ;
- Les accès aux traitements de données nécessitent une authentification des personnes accédant aux données, au moyen d'un identifiant et d'un mot de passe individuels, suffisamment robustes et régulièrement renouvelés, ou par tout autre moyen d'authentification de même fiabilité ;
- Les conditions d'administration du système d'information prévoient l'existence de systèmes automatiques de traçabilité (journaux, audits…).

Les mesures de sécurité pour le site internet :

- Le responsable de traitement prend les mesures nécessaires pour se prémunir contre toute atteinte à la confidentialité des données traitées. Les données transitant sur des canaux de communication non sécurisés doivent notamment faire l'objet de mesures techniques visant à les rendre incompréhensibles à toute personne non autorisée à y avoir accès.

Les mesures de sécurité pour les données de santé :

- Le responsable de traitement s'engage à respecter les dispositions prévues par le code de bonne conduite annexé à la convention AERAS[12] concernant la collecte et l'utilisation de données relatives à l'état de santé en vue de la souscription ou de l'exécution d'un contrat d'assurance.

(12) Un code de bonne conduite sur l'utilisation des données relatives à l'état de santé a été établi dans le cadre de la convention AERAS (1er février 2011). Il concerne la collecte et l'utilisation des données relatives à l'état de santé en vue de la souscription ou l'exécution d'un contrat d'assurance. Ce code précise les conditions de stricte confidentialité dans lesquelles les données relatives à l'état de santé des assurés doivent être traitées.

Transferts de données hors UE

Certains transferts de données à caractère personnel peuvent être réalisés vers des pays tiers à l'UE et n'assurant pas un niveau de protection adéquat, lorsque :

- Il existe un niveau suffisant de protection de la vie privée ainsi que des droits et libertés des personnes ou que ces transferts sont juridiquement encadrés (ex : CCT ou BCR) ;
- Le responsable de traitement a clairement informé les personnes de l'existence d'un transfert de données vers des pays tiers, ou s'engage, sur simple demande de la personne concernée, à apporter une information complète sur la finalité, les données, les destinataires et les moyens mis en œuvre pour encadrer ce transfert ;
- Les transferts sont réalisés dans le cadre de l'exécution des contrats ou de la sauvegarde de la vie humaine pour la mise en œuvre des garanties d'assistance ;
- Les transferts sont réalisés lors de la gestion des actions ou contentieux liés à l'activité de l'entreprise (ex : constatation, exercice ou défense de ses droits en justice ou pour les besoins de défense des personnes concernées).

Les transferts répétitifs, massifs ou structurels de données personnelles doivent faire l'objet d'un encadrement juridique spécifique (niveau de protection adéquat, safe Harbor, CCT, BCR…). Ces transferts d'informations dans le cadre de la passation, la gestion et l'exécution des contrats ayant été expressément prévue par la NS16 aucune autorisation de la CNIL n'est nécessaire, à condition que ces transferts restent impérativement dans le champ de la NS. À défaut, ils doivent faire l'objet de formalités préalables auprès de la CNIL dans les conditions prévues par ladite loi.

Le responsable de traitement s'engage, sur simple demande de la personne concernée, à apporter une information complète sur la finalité, les données, les destinataires et les moyens mis en œuvre pour encadrer ce transfert.